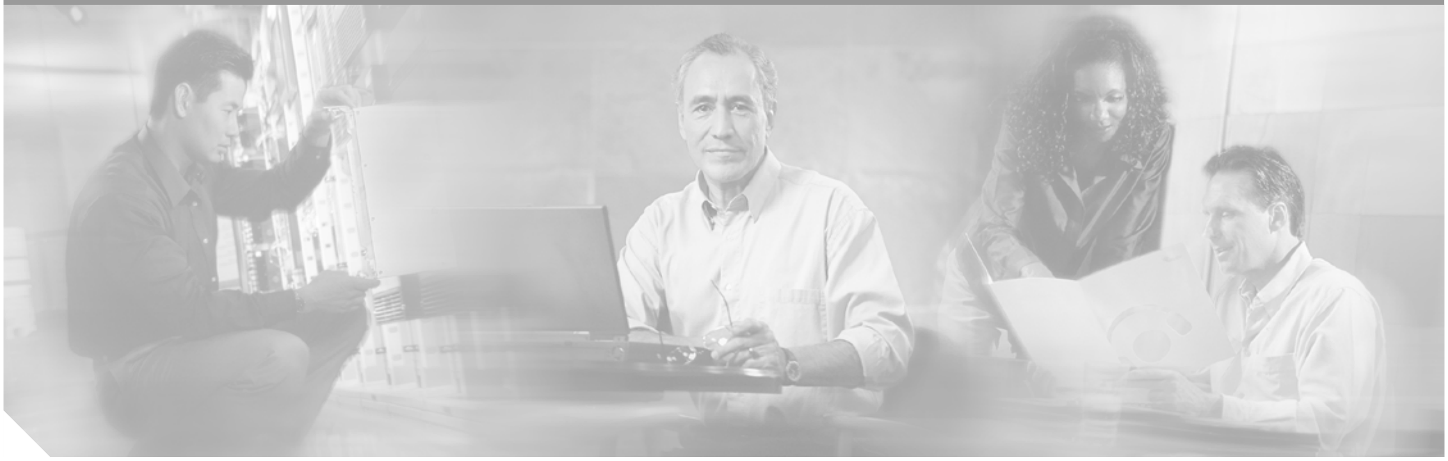


Cisco ONS 15327 Procedure Guide

Product and Documentation Release 3.4
Last Updated: November 10, 2004

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

Customer Order Number: DOC-7815640=
Text Part Number: 78-15640-01

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.

Cisco ONS 15327 Procedure Guide

CONTENTS

About this Guide xxxi

Document Objectives xxxi

Audience xxxi

Document Organization xxxii

Chapter (Director Level) xxxii

Non-Trouble Procedure (NTP) xxxii

Detailed Level Procedure (DLP) xxxii

Related Documentation xxxiii

Document Conventions xxxiii

Where to Find Safety and Warning Information xxxiv

Obtaining Documentation xxxiv

Cisco.com xxxiv

Documentation CD-ROM xxxiv

Ordering Documentation xxxiv

Documentation Feedback xxxv

Obtaining Technical Assistance xxxv

Cisco.com xxxv

Technical Assistance Center xxxvi

Cisco TAC Website xxxvi

Cisco TAC Escalation Center xxxvi

Obtaining Additional Publications and Information xxxvii

CHAPTER 1 Install Hardware 1-1

Before You Begin 1-1

Required Tools and Equipment 1-2

Included Materials 1-2

User-Supplied Materials 1-3

Tools Needed 1-3

Test Equipment 1-3

NTP-B 1 Unpack and Inspect the ONS 15327 Shelf Assembly 1-4

DLP-B 1 Unpack and Verify the Shelf Assembly 1-4

DLP-B 2 Inspect the Shelf Assembly 1-5

NTP-B 2 Install the Shelf Assembly 1-5

DLP-B 3 Reverse the Mounting Bracket to Fit a 19-inch Rack 1-6

DLP-B 5 Mount the ONS 15327 in a Rack 1-8
DLP-B 7 Mount Multiple Shelf Assemblies in a Rack 1-8
DLP-B 329 Install the Tie-Down Bar 1-9
NTP-B 216 Install the Mechanical Interface Cards 1-11
NTP-B 6 Install the Power and Ground 1-12
DLP-B 16 Connect the Office Ground to the ONS 15327 1-13
DLP-B 17 Connect Office Power to the ONS 15327 Shelf (Screw-Lock Power Connector) 1-14
DLP-B 18 Turn On and Verify Office Power 1-19
DLP-B 30 Install Ferrites on Power Cabling 1-20
NTP-B 7 Install the Fan-Tray Assembly 1-20
NTP-B 217 Install the XTCs 1-21
NTP-B 218 Install the Optical and Ethernet Cards 1-23
DLP-D 4 Install SFP Connectors on G1000-2 Cards 1-24
DLP-D 6 Remove SFP Connectors from G1000-2 Cards 1-25
NTP-B 219 Remove and Replace a Card 1-26
DLP-B 320 Delete a Card 1-26
DLP-B 247 Change an Optical Card 1-27
NTP-B 115 Preprovision a Slot 1-28
NTP-B 8 Install Wires to Alarm, Timing, LAN, and Craft Pin Connections 1-28
DLP-B 321 Install External Alarm Cables 1-29
DLP-B 322 Install Timing Cables 1-30
DLP-B 323 Install the Serial Cable for TL1 Craft Interface 1-32
NTP-B 220 Install the Electrical Cables 1-33
DLP-B 324 Install DS-1 Champ Cables on a MIC 1-34
DLP-B 325 Install Coaxial Cable With BNC Connectors 1-38
DLP-B 326 Route Electrical Cables 1-39
NTP-B 221 Install Optical Cables 1-40
DLP-B 327 Install Fiber-Optic Cables on the LGX Interface 1-42
DLP-B 42 Install Fiber-Optic Cables on OC-N Cards 1-42
DLP-B 43 Install Fiber-Optic Cables for UPSR Configurations 1-43
DLP-B 44 Install Fiber-Optic Cables for BLSR Configurations 1-46
DLP-B 46 Route Fiber-Optic Cables 1-47
NTP-B 13 Perform the Shelf Installation Acceptance Test 1-48
DLP-B 33 Measure Voltage 1-49

CHAPTER 2 Connect the PC and Log into the GUI 2-1
Before You Begin 2-1
NTP-B 21 Set Up Computer for CTC 2-1

DLP-B 47 Run the CTC Installation Wizard for Windows 2-2
DLP-B 48 Run the CTC Installation Wizard for UNIX 2-5
DLP-B 49 Set Up the Java Runtime Environment for UNIX 2-7
NTP-B 22 Set Up CTC Computer to Connect to the ONS 15327 2-8
DLP-B 50 Set Up a Windows PC for Craft Connection to an ONS 15327 on the Same Subnet Using Static IP Addresses 2-11
DLP-B 51 Set Up a Windows PC for Craft Connection to an ONS 15327 Using DHCP 2-13
DLP-B 52 Set Up a Windows PC for Craft Connection to an ONS 15327 Using Automatic Host Detection 2-15
DLP-B 53 Set Up a Solaris Workstation for a Craft Connection to an ONS 15327 2-17
DLP-B 55 Set Up a Computer for a Corporate LAN Connection 2-19
DLP-B 56 Disable Proxy Service Using Internet Explorer (Windows) 2-20
DLP-B 57 Disable Proxy Service Using Netscape (Windows and UNIX) 2-20
DLP-B 58 Provision Remote Access to the ONS 15327 2-21
NTP-B 23 Log into the ONS 15327 GUI 2-22
DLP-B 59 Connect Computer to the ONS 15327 2-22
DLP-B 60 Log into CTC 2-23
DLP-B 61 Create Login Node Groups 2-25
DLP-B 62 Add a Node to the Current Session or Login Group 2-26

CHAPTER 3 Turn Up Node 3-1
Before You Begin 3-1
NTP-B 24 Verify Card Installation 3-2
NTP-B 30 Create Users and Assign Security 3-3
DLP-B 74 Create a New User - Single Node 3-3
DLP-B 75 Create a New User - Multiple Nodes 3-4
NTP-B 25 Set Up Name, Date, Time, and Contact Information 3-5
NTP-B 169 Set Up CTC Network Access 3-7
DLP-B 249 Provision IP Settings 3-7
DLP-B 65 Create a Static Route 3-9
DLP-B 250 Set Up or Change Open Shortest Path First Protocol 3-10
DLP-B 251 Set Up or Change Routing Information Protocol 3-12
NTP-B 27 Set Up the ONS 15327 for Firewall Access 3-13
DLP-B 67 Provision the IIOP Listener Port on the ONS 15327 3-14
DLP-B 68 Provision the IIOP Listener Port on the CTC Computer 3-16
NTP-B 28 Set Up Timing 3-16
DLP-B 69 Set Up External or Line Timing 3-17
DLP-B 70 Set Up Internal Timing 3-19
NTP-B 170 Create Optical Protection Groups 3-20

NTP-B 171 Set Up SNMP 3-21

NTP-B 34 Create Ethernet RMON Alarm Thresholds 3-23

CHAPTER 4 **Turn Up Network** 4-1

Before You Begin 4-1

NTP-B 35 Verify Node Turn Up 4-2

NTP-B 124 Provision a Point-to-Point Network 4-3

DLP-B 253 Provision SONET DCC Terminations 4-4

DLP-B 214 Change the Service State for a Port 4-5

NTP-B 173 Point-to-Point Network Acceptance Test 4-6

DLP-B 254 XTC Active/Standby Switch Test 4-7

DLP-B 88 Optical 1+1 Protection Test 4-8

NTP-B 38 Provision a Linear ADM Network 4-10

NTP-B 174 Linear ADM Network Acceptance Test 4-11

NTP-B 40 Provision BLSR Nodes 4-13

NTP-B 126 Create a BLSR 4-14

NTP-B 175 BLSR Acceptance Test 4-16

DLP-B 217 BLSR Exercise Ring Test 4-18

DLP-B 91 BLSR Ring Switch Test 4-19

NTP-B 44 Provision UPSR Nodes 4-22

NTP-B 177 UPSR Acceptance Test 4-23

DLP-B 94 UPSR Protection Switching Test 4-25

NTP-B 46 Subtend a UPSR from a BLSR 4-25

NTP-B 47 Subtend a BLSR from a UPSR 4-27

NTP-B 48 Subtend a BLSR from a BLSR 4-27

CHAPTER 5 **Create Circuits and VT Tunnels** 5-1

Before You Begin 5-1

NTP-B 127 Verify Network Turn Up 5-3

NTP-B 181 Create an Automatically Routed DS-1 Circuit 5-5

NTP-B 182 Create a Manually Routed DS-1 Circuit 5-9

NTP-B 183 Create a Unidirectional DS-1 Circuit with Multiple Drops 5-11

DLP-B 314 Assign a Name to a Port 5-14

DLP-B 95 Provision a DS-1 Circuit Source and Destination 5-15

NTP-B 184 Create an Automatically Routed DS-3 Circuit 5-16

NTP-B 185 Create a Manually Routed DS-3 Circuit 5-20

NTP-B 186 Create a Unidirectional DS-3 Circuit with Multiple Drops 5-22

DLP-B 218 Provision UPSR Selectors During Circuit Creation 5-25
DLP-B 208 Provision a DS-3 Circuit Source and Destination 5-26
DLP-B 96 Provision a DS-1 or DS-3 Circuit Route 5-27
NTP-B 133 Create an Automatically Routed VT Tunnel 5-28
NTP-B 134 Create a Manually Routed VT Tunnel 5-30
DLP-B 219 Provision a VT Tunnel Route 5-32
NTP-B 135 Test Electrical Circuits 5-33
NTP-B 188 Create an Automatically Routed Optical Circuit 5-35
NTP-B 189 Create a Manually Routed Optical Circuit 5-38
NTP-B 190 Create a Unidirectional Optical Circuit with Multiple Drops 5-41
DLP-B 97 Provision an Optical Circuit Source and Destination 5-44
DLP-B 98 Provision an Optical Circuit Route 5-45
NTP-B 62 Test Optical Circuits 5-46
NTP-B 191 Create an E-Series EtherSwitch Circuit (Multicard or Single-Card Mode) 5-48
NTP-B 192 Create a Circuit for an E-Series Card in Port-Mapped Mode 5-50
NTP-B 142 Create an E-Series Shared Packet Ring Ethernet Circuit 5-52
NTP-B 143 Create an E-Series Hub and Spoke Ethernet Configuration 5-55
NTP-B 144 Create an E-Series Single-Card EtherSwitch Manual Cross-Connect 5-57
NTP-B 145 Create an E-Series Multicard EtherSwitch Manual Cross-Connect 5-60
DLP-B 99 Determine Available VLANs 5-63
DLP-B 246 Provision E-Series Ethernet Card Mode 5-64
DLP-B 220 Provision E-Series Ethernet Ports 5-64
DLP-B 221 Provision E-Series Ethernet Ports for VLAN Membership 5-65
NTP-B 146 Test E-Series Circuits 5-67
NTP-B 147 Create a G-Series Circuit 5-68
NTP-B 148 Create a Manual Cross-Connect for a G-Series or an E-Series in Port-Mapped Mode 5-70
DLP-B 222 Provision G-Series Ethernet Ports 5-72
NTP-B 149 Test G-Series Circuits 5-73
NTP-B 194 Create Overhead Circuits 5-74
DLP-B 313 Create a DCC Tunnel 5-75
DLP-B 212 Create a User Data Channel 5-76

CHAPTER 6 Manage Alarms 6-1
Before You Begin 6-1
NTP-B 195 Document Existing Provisioning 6-2
DLP-B 138 Print CTC Data 6-2
DLP-B 139 Export CTC Data 6-3

NTP-B 196 View Alarms, History, Events, and Conditions 6-5
DLP-B 110 View Alarm History 6-7
DLP-B 111 Changing the Maximum Number of Session Entries for Alarm History 6-9
DLP-B 112 Display Alarms and Conditions Using Time Zone 6-10
DLP-B 113 Synchronize Alarms 6-10
DLP-B 114 View Conditions 6-11
NTP-B 68 Delete Cleared Alarms from Display 6-12
NTP-B 69 View Alarm-Affected Circuits 6-13
NTP-B 70 Create, Download, and Assign Alarm Severity Profiles 6-15
DLP-B 115 Create Alarm Severity Profiles 6-16
DLP-B 223 Download an Alarm Severity Profile 6-19
DLP-B 116 Apply Alarm Profiles to Ports 6-20
DLP-B 117 Apply Alarm Profiles to Cards and Nodes 6-23
DLP-B 118 Delete Alarm Severity Profiles 6-24
NTP-B 168 Enable, Modify, or Disable Alarm Severity Filtering 6-25
DLP-B 225 Enable Alarm Filtering 6-26
DLP-B 226 Modify Alarm and Condition Filtering Parameters 6-27
DLP-B 227 Disable Alarm Filtering 6-29
NTP-B 72 Suppress and Discontinue Alarm Suppression 6-29
DLP-B 119 Suppress Alarm Reporting 6-30
DLP-B 120 Discontinue Alarm Suppression 6-31
NTP-B 32 Provision External Alarms and Controls on the XTC 6-32

CHAPTER 7 Monitor Performance 7-1
Before You Begin 7-1
NTP-B 73 Enable Performance Monitoring 7-2
DLP-B 121 Enable Pointer Justification Count Performance Monitoring 7-2
DLP-B 122 Enable Intermediate-Path Performance Monitoring 7-4
NTP-B 195 Monitor Electrical or Optical Performance 7-6
DLP-B 123 View Electrical PM Parameters 7-7
DLP-B 261 Refresh PM Counts for a Different Port 7-8
DLP-B 124 Refresh Electrical or Optical PM Counts at Fifteen-Minute Intervals 7-8
DLP-B 318 Refresh Electrical or Optical PM Counts at One-Day Intervals 7-9
DLP-B 126 Monitor Near-End PM Counts 7-10
DLP-B 127 Monitor Far-End PM Counts 7-10
DLP-B 129 Reset Current PM Counts 7-11
DLP-B 130 Clear Selected PM Counts 7-11
DLP-B 260 Set Auto-Refresh Interval for Displayed PM Counts 7-12
DLP-B 317 View Optical OC-N PM Parameters 7-13

DLP-B 319 Monitor PM Counts for Selected Signal Types 7-14

NTP-B 198 Monitor Ethernet Performance 7-15

DLP-B 256 View Ethernet Statistics PM Parameters 7-16

DLP-B 257 View Ethernet Utilization PM Parameters 7-17

DLP-B 259 Refresh Ethernet PM Counts at a Different Time Interval 7-18

DLP-B 258 View Ethernet History PM Parameters 7-18

CHAPTER 8 **Manage Circuits** 8-1

Before You Begin 8-1

NTP-B 199 Locate and View Circuits 8-3

DLP-B 262 Filter the Display of Circuits 8-4

DLP-B 131 Search for Circuits 8-5

DLP-B 229 View Circuits on a Span 8-6

NTP-B 151 Modify Circuit Characteristics 8-7

DLP-B 230 Change a Circuit State 8-7

DLP-B 231 Edit a Circuit Name 8-8

DLP-B 232 Change Active and Standby Span Color 8-9

DLP-B 233 Edit UPSR Circuit Path Selectors 8-10

NTP-B 416 Convert a CTC Circuit to TL1 Cross-Connects 8-11

NTP-B 417 Upgrade TL1 Cross-Connects to CTC Circuits 8-13

NTP-B 152 Delete Circuits 8-13

NTP-B 78 Create a Monitor Circuit 8-14

NTP-B 79 Create a J1 Path Trace 8-15

DLP-B 264 Provision Path Trace on Circuit Source and Destination Ports 8-16

DLP-B 137 Provision Path Trace on OC-N Ports 8-19

CHAPTER 9 **Change Port Settings** 9-1

Before You Begin 9-1

NTP-B 88 Modify Line Settings and PM Parameter Thresholds for Electrical Ports 9-1

DLP-B 165 Change Line and Threshold Settings for the DS-1 Ports 9-2

DLP-B 166 Change Line and Threshold Settings for the DS-3 Ports 9-6

NTP-B 89 Modify Line Settings and PM Parameter Thresholds for Optical Ports 9-9

DLP-B 170 Change Line Settings for OC-N Cards 9-9

DLP-B 171 Change SONET Thresholds Settings for OC-N Cards 9-11

DLP-B 172 Change an Optical Port to SDH 9-14

CHAPTER 10 **Change Node Settings** 10-1

Before You Begin 10-1

NTP-B 81 Change Node Management Information 10-2

DLP-B 140 Change the Node Name, Date, Time, and Contact Information 10-2

DLP-B 265 Change the Login Legal Disclaimer 10-3

NTP-B 201 Change CTC Network Access 10-4

DLP-B 266 Change IP Settings 10-5

DLP-B 142 Modify a Static Route 10-6

DLP-B 143 Delete a Static Route 10-6

DLP-B 144 Disable the Open Shortest Path First Protocol 10-7

NTP-B 202 Customize the CTC Network View 10-7

DLP-B 145 Change the Network View Background Color 10-8

DLP-B 267 Change the Default Network View Background Map 10-8

DLP-B 268 Apply a Custom Network View Background Map 10-9

DLP-B 148 Create Domain Icons 10-10

DLP-B 149 Manage Domain Icons 10-10

DLP-B 269 Enable Dialog Box Do-Not-Display Option 10-11

NTP-B 203 Modify or Delete 1+1 Card Protection Settings 10-12

DLP-B 154 Modify a 1+1 Protection Group 10-13

DLP-B 155 Delete a Protection Group 10-14

NTP-B 204 Delete a SONET DCC Termination 10-14

NTP-B 85 Change Node Timing 10-15

DLP-B 157 Change the Node Timing Source 10-15

NTP-B 205 Modify Users and Change Security 10-17

DLP-B 271 Change Node Security Policy - Single Node 10-17

DLP-B 272 Change Node Security Policy - Multiple Nodes 10-18

DLP-B 158 Change User and Security Settings - Single Node 10-19

DLP-B 160 Change User and Security Settings - Multiple Nodes 10-20

DLP-B 315 Log Out a User - Single Node 10-20

DLP-B 316 Log Out a User - Multiple Nodes 10-21

DLP-B 159 Delete User - Single Node 10-22

DLP-B 161 Delete User - Multiple Nodes 10-22

NTP-B 87 Change SNMP Settings 10-23

DLP-B 273 Modify SNMP Trap Destination 10-24

DLP-B 163 Delete SNMP Trap Destinations 10-25

DLP-B 164 Delete Ethernet RMON Alarm Thresholds 10-25

CHAPTER 11 Upgrade Cards and Spans 11-1

Before You Begin 11-1

NTP-B 229 Upgrade the XTC-14 Card to XTC-28 Card 11-1

NTP-B 94 Upgrade Optical Spans Automatically 11-3

NTP-B 95 Upgrade Optical Spans Manually 11-5

DLP-B 293 Perform a Manual Span Upgrade on a Two-Fiber BLSR 11-6

DLP-B 295 Perform a Manual Span Upgrade on a UPSR 11-8

DLP-B 296 Perform a Manual Span Upgrade on a 1+1 Protection Group 11-9

DLP-B 297 Perform a Manual Span Upgrade on an Unprotected Span 11-11

CHAPTER 12 Convert Network Configurations 12-1

Before You Begin 12-1

NTP-B 154 Convert a Point-to-Point to a Linear ADM 12-1

DLP-B 298 Check the Network for Alarms and Conditions 12-3

NTP-B 155 Convert a Point-to-Point or a Linear ADM to a Two-Fiber BLSR 12-3

DLP-B 189 Verify that a 1+1 Working Slot is Active 12-5

NTP-B 156 Convert a Point-to-Point or Linear ADM to a UPSR 12-6

NTP-B 210 Convert a USPR to a Two-Fiber BLSR 12-6

NTP-B 159 Modify a BLSR 12-8

DLP-B 301 Initiate a BLSR Manual Ring Switch 12-9

DLP-B 241 Clear a BLSR Manual Ring Switch 12-10

CHAPTER 13 Add and Remove Nodes 13-1

Before You Begin 13-1

NTP-B 12 Add a BLSR Node 13-2

DLP-B 302 Check BLSR or UPSR Alarms and Conditions 13-5

DLP-B 242 Create a BLSR on a Single Node 13-6

DLP-B 303 Initiate a BLSR Force Ring Switch 13-6

DLP-B 194 Clear a BLSR Force Ring Switch 13-8

NTP-B 213 Remove a BLSR Node 13-9

DLP-B 304 Verify BLSR Pass-Through Circuits 13-11

DLP-B 195 Verify Timing in a Reduced Ring 13-12

DLP-B 196 Delete a BLSR from a Single Node 13-12

NTP-B 105 Add a UPSR Node 13-13

NTP-B 106 Remove a UPSR Node 13-15

DLP-B 197 Initiate a UPSR Force Switch 13-16

DLP-B 198 Clear a UPSR Switch 13-17

CHAPTER 14 Maintain the Node 14-1

Before You Begin 14-1

NTP-B 107 Inspect and Maintain the Air Filter 14-2

DLP-B 199 Inspect, Clean, and Replace the Reusable Air Filter 14-2
DLP-B 200 Inspect and Replace the Disposable Air Filter 14-4
NTP-B 108 Back Up the Database 14-6
NTP-B 109 Restore the Database 14-8
NTP-B 163 Restore the Node to Factory Configuration 14-10
DLP-B 244 Use the Reinitialization Tool to Clear the Database and Upload Software (Windows) 14-11
DLP-B 245 Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX) 14-13
NTP-B 214 Offload the Security Audit Trail Log 14-15
NTP-B 110 Inhibit Protection Switching 14-16
DLP-B 201 Apply a Lock On 14-16
DLP-B 202 Apply a Lock Out 14-17
DLP-B 203 Clear a Lock On or Lock Out 14-18
NTP-B 111 Revert to an Earlier Software Load 14-19
NTP-B 112 Clean Fiber Connectors 14-20
DLP-B 204 Scope and Clean Fiber Connectors and Adapters with Alcohol and Dry Wipes 14-21
DLP-B 205 Clean Fiber Connectors with CLETOP 14-21
DLP-B 206 Clean the Fiber Adapters 14-22
NTP-B 113 Reset the XTC Using CTC 14-23
NTP-B 215 View G1000-2 Ethernet Maintenance Information 14-24
DLP-B 306 View Loopback Status 14-24
DLP-B 307 View Ethernet Bandwidth Usage 14-25
NTP-B 228 View E10/100-4 Ethernet Maintenance Information 14-25
DLP-B 309 View Ethernet MAC Address Table 14-26
DLP-B 310 View Ethernet Trunk Utilization 14-26
NTP-B 225 Switch the Node Timing Reference 14-27
DLP-B 330 Manual or Force Switch the Node Timing Reference 14-27
DLP-B 331 Clear a Manual or Force Switched Node Timing Reference 14-28

CHAPTER 15 **Power Down the Node** 15-1

NTP-B 114 Power Down the ONS 15327 15-1

APPENDIX A **CTC Information and Shortcuts** A-1

Displaying Node, Card, and Network Views A-1
Manage the CTC Window A-2
CTC Menu and Toolbar Options A-2
CTC Mouse Options A-5
Node View Shortcuts A-6

Network View Tasks A-6
Table Display Options A-7
Equipment Inventory A-8

APPENDIX B

Shelf Assembly Specifications B-1
Bandwidth B-1
Slot Assignments B-1
Cards B-1
Configurations B-2
Cisco Transport Controller B-2
External LAN Interface B-2
TL1 Craft Interface B-2
Modem Interface B-2
Alarm Interface B-2
Nonvolatile Memory B-3
BITS Interface B-3
System Timing B-3
Power Specifications B-3
Environmental Specifications B-3
Dimensions B-3

APPENDIX C

Network Element Defaults C-1
Network Element Defaults Description C-1
NTP-B 164 Edit Network Element Defaults C-2
NTP-B 165 Import Network Element Defaults C-3
NTP-B 166 Export Network Element Defaults C-4
Card Default Settings C-4
Node Default Settings C-14

APPENDIX D

Alternate Installation Procedures D-1
Before You Begin D-1
NTP-B 223 Install the Fiber-Optic Cable Storage Drawer D-2
NTP-B 224 Route Cables Through the Fiber-Optic Cable Storage Drawer D-2
NTP-B 222 Connect Office Power to the ONS 15327 Shelf (Terminal-Lug Power Connector) D-4

GLOSSARY

INDEX

FIGURES

Figure 1-1 Reversing the Mounting Brackets (23-Inch Position to 19-Inch Position) **1-7**

Figure 1-2 Tie-Down Bar **1-10**

Figure 1-3 ONS 15327 Slot Numbering **1-11**

Figure 1-4 Removing the MIC Power Connector **1-16**

Figure 1-5 Inserting a Power Cable into the MIC Power Connector **1-17**

Figure 1-6 Installing the MIC Power Connector **1-18**

Figure 1-7 Redundant Power Connections **1-18**

Figure 1-8 Installing the Fan-Tray Assembly **1-21**

Figure 1-9 Installing an XTC (XTC 28-3) **1-22**

Figure 1-10 Installing an Ethernet Card (E10/100-T) **1-24**

Figure 1-11 Pins 1 and 8 on the RJ-45 Connector **1-30**

Figure 1-12 BITS In Pins on the RJ-45 Connector **1-31**

Figure 1-13 BITS Out Pins on the RJ-45 Connector **1-31**

Figure 1-14 Straight DS-1 Cable **1-36**

Figure 1-15 Right-Angle DS-1 Cable **1-37**

Figure 1-16 Installing a Straight DS-1 Cable **1-38**

Figure 1-17 Installing a Coaxial Cable with BNC Connectors **1-39**

Figure 1-18 Installing a Fiber-Optic Cable **1-41**

Figure 1-19 Connecting Fiber to a Four-Node UPSR **1-44**

Figure 1-20 Connecting Fiber to an Eight-Node Traditional UPSR Dual-Ring Interconnect **1-45**

Figure 1-21 Connecting Fiber to a Four-Node, Two-Fiber BLSR **1-47**

Figure 2-1 Cisco Transport Controller Installation Wizard **2-3**

Figure 2-2 Logging into CTC **2-24**

Figure 2-3 Login Node Group **2-26**

Figure 3-1 ONS 15327 Nodes Residing Behind a Firewall **3-14**

Figure 3-2 A CTC Computer and ONS 15327s Residing Behind Firewalls **3-14**

Figure 3-3 Setting SNMP **3-22**

Figure 3-4 SNMP Trap Destinations **3-22**

Figure 3-5 Creating RMON Thresholds **3-23**

Figure 4-1 Linear ADM Configuration **4-10**

Figure 4-2 Four-Node, Two-Fiber BLSR Fiber Connection Example **4-13**

Figure 4-3 Setting BLSR Properties **4-14**

Figure 4-4 UPSR Fiber Connection Example **4-22**

Figure 4-5 UPSR Subtended from a BLSR **4-26**

Figure 4-6 BLSR Subtended from a BLSR **4-28**

Figure 5-1 Setting Circuit Attributes For a DS-1 Circuit **5-7**

Figure 5-2 Setting Circuit Routing Preferences for a DS-1 Circuit **5-8**

Figure 5-3 Setting Circuit Attributes for a Unidirectional DS-1 Circuit **5-13**

Figure 5-4 Setting Circuit Attributes for a DS-3 **5-17**

Figure 5-5 Setting Circuit Routing Preferences for a DS-3 Circuit **5-18**

Figure 5-6 Setting Circuit Attributes for a Unidirectional DS-3 Circuit **5-23**

Figure 5-7 Setting Attributes for a VT Tunnel **5-29**

Figure 5-8 Manually Routing a VT Tunnel **5-32**

Figure 5-9 Setting Circuit Attributes for an Optical Circuit **5-36**

Figure 5-10 Setting Circuit Routing Preferences for an Optical Circuit **5-37**

Figure 5-11 Manually Routing an OC-N Circuit **5-45**

Figure 5-12 Provisioning a DCC Tunnel **5-76**

Figure 6-1 Selecting CTC Data For Print **6-3**

Figure 6-2 Selecting CTC Data For Export **6-4**

Figure 6-3 ONS 15327 CTC Node (Login) View **6-6**

Figure 6-4 CTC Preferences Dialog Box **6-9**

Figure 6-5 Node View Conditions Window **6-11**

Figure 6-6 Select Affected Circuits Option **6-14**

Figure 6-7 Viewing an Alarm-Affected Circuit **6-15**

Figure 6-8 Network View Alarm Profiles Window **6-17**

Figure 6-9 Store Profile(s) Dialog Box **6-18**

Figure 6-10 Card View Optical Port Alarm Profile **6-21**

Figure 6-11 Card View Electrical Port Alarm Profile **6-22**

Figure 6-12 Node View Alarm Profile **6-23**

Figure 6-13 Select Node/Profile Combination For Delete Dialog Box **6-24**

Figure 6-14 Alarm Filter Dialog Box General Tab **6-27**

Figure 6-15 Alarm Filter Dialog Box Conditions Tab **6-28**

Figure 6-16 XTC Card External Alarms **6-33**

Figure 7-1 Line Tab for Enabling Pointer Justification Count Parameters **7-3**

Figure 7-2 Viewing Pointer Justification Counts **7-4**

Figure 7-3 SONET STS Tab for Enabling IPPM **7-5**

Figure 7-4 Viewing Electrical Performance Monitoring Information **7-7**
Figure 7-5 Viewing Optical Performance Monitoring Information **7-13**
Figure 7-6 Statistics Window on the Card View Performance Tab **7-16**
Figure 7-7 Utilization Window on the Card View Performance Tab **7-17**
Figure 7-8 History Window on the Card View Performance Tab **7-19**
Figure 8-1 Changing Circuit State **8-8**
Figure 8-2 Editing UPSR Path Selectors **8-11**
Figure 8-3 Choosing the Cross-Connects Only Option **8-12**
Figure 8-4 Setting Up a Path Trace **8-18**
Figure 8-5 Detailed Circuit Window With Manual Expected String Enabled **8-19**
Figure 9-1 Provisioning Line Parameters on the DS-1 Ports **9-3**
Figure 9-2 Provisioning SONET Thresholds for the OC48 IR 1310 Card **9-12**
Figure 11-1 Resetting the XTC card **11-2**
Figure 13-1 Three-Node Two-Fiber BLSR Before a Fourth Node Is Added **13-2**
Figure 13-2 Four-Node, Two-Fiber BLSR Before a Node Is Removed **13-10**
Figure 13-3 Circuits on Span Dialog Box with a Force Switch **13-17**
Figure 14-1 Removing the Reusable Fan-Tray Air Filter **14-3**
Figure 14-2 Replacing the Reusable Fan-Tray Air Filter **14-4**
Figure 14-3 Removing the Disposable Fan-Tray Air Filter **14-5**
Figure 14-4 Replacing the Disposable Fan-Tray Air Filter **14-5**
Figure 14-5 Backing Up the XTC Database **14-7**
Figure 14-6 Confirming the Database Backup **14-7**
Figure 14-7 Restoring the XTC Database **14-9**
Figure 14-8 Restoring the Database—Traffic Loss Warning **14-9**
Figure 14-9 Restoring the Database—In-Process Notification **14-10**
Figure 14-10 Reinitialization Tool in Windows **14-12**
Figure 14-11 Confirm NE Restoration **14-13**
Figure 14-12 Reinitialization Tool in UNIX **14-14**
Figure D-1 Opening the Fiber-Optic Cable Storage Drawer **D-3**
Figure D-2 Locking the Cable Storage Drawer **D-3**
Figure D-3 MIC Terminal-Lug Power Connector **D-6**
Figure D-4 Power Cable Inserted into the MIC Terminal-Lug Power Connector **D-7**
Figure D-5 Redundant Power Connected to an ONS 15327 **D-8**

TABLES

Table 1-1 Alarm Input Pin Assignments **1-29**

Table 1-2 Alarm (External Control) Output Pin Assignments **1-30**

Table 1-3 BITS Cable Pin Assignments **1-31**

Table 1-4 External Timing Pin Assignments for BITS **1-32**

Table 1-5 Pin Assignments for Champ Connector (the shaded area corresponds to the white/orange binder group) **1-34**

Table 1-6 Optical Transmit and Receive Levels **1-41**

Table 1-7 ONS 15327 Shelf Installation Task Summary **1-48**

Table 2-1 ONS 15327 Connection Methods **2-9**

Table 2-2 ONS 15327 Craft Connection Options **2-10**

Table 3-1 Ports Used by the XTC Cards **3-15**

Table 3-2 Ethernet Threshold Variables (MIBs) **3-24**

Table 5-1 ONS 15327 Circuit Options **5-2**

Table 5-2 CTC Circuit Source and Destination Options For VT Circuits **5-2**

Table 5-3 CTC Circuit Source and Destination Options for STS Circuits **5-3**

Table 5-4 VLAN Settings **5-66**

Table 6-1 Alarm Column Descriptions **6-6**

Table 6-2 Color Codes for Alarms and Conditions **6-7**

Table 7-1 Traffic Cards that Terminate the Line (LTEs) **7-2**

Table 8-1 ONS 15327 Circuit Status **8-2**

Table 8-2 ONS 15327 Circuit States **8-3**

Table 8-3 ONS 15327 Cards Capable of Path Trace **8-16**

Table 9-1 Line Options for DS-1 Ports **9-4**

Table 9-2 Line Thresholds Options for DS-1 Ports **9-4**

Table 9-3 Electrical Path Threshold Options for DS-1 Ports **9-5**

Table 9-4 VT1.5 Path Thresholds Options for DS-1 ports **9-6**

Table 9-5 Line Options for DS-3 Ports **9-7**

Table 9-6 Line Threshold Options for DS-3 Ports **9-8**

Table 9-7 STS-1 Path Threshold Options for DS-3 Ports **9-8**

Table 9-8 OC-N Card Line Settings **9-10**

Table 9-9 OC-N SONET Thresholds Options **9-12**

Table 10-1 Managing Domains **10-11**

Table A-1 Change CTC Views **A-1**

Table A-2 CTC Menu and Toolbar Options **A-2**

Table A-3 CTC Window Mouse Shortcuts **A-5**

Table A-4 Performing Node View Card Shortcuts **A-6**

Table A-5 Network Management Tasks in Network View **A-6**

Table A-6 Table Display Options **A-7**

Table C-1 DS-1 Default Settings **C-5**

Table C-2 DS-3 Default Settings **C-7**

Table C-3 OC-3 Card Default Settings **C-8**

Table C-4 OC-12 Card Default Settings **C-10**

Table C-5 OC-48 Cards Default Settings **C-12**

Table C-6 Node Default Settings **C-14**

PROCEDURES

CHAPTER 1 **Install Hardware** 1-1

NTP-B1 Unpack and Inspect the ONS 15327 Shelf Assembly 1-4
NTP-B2 Install the Shelf Assembly 1-5
NTP-B216 Install the Mechanical Interface Cards 1-11
NTP-B6 Install the Power and Ground 1-12
NTP-B7 Install the Fan-Tray Assembly 1-20
NTP-B217 Install the XTCs 1-21
NTP-B218 Install the Optical and Ethernet Cards 1-23
NTP-B219 Remove and Replace a Card 1-26
NTP-B115 Preprovision a Slot 1-28
NTP-B8 Install Wires to Alarm, Timing, LAN, and Craft Pin Connections 1-28
NTP-B220 Install the Electrical Cables 1-33
NTP-B221 Install Optical Cables 1-40
NTP-B13 Perform the Shelf Installation Acceptance Test 1-48

CHAPTER 2 **Connect the PC and Log into the GUI** 2-1

NTP-B21 Set Up Computer for CTC 2-1
NTP-B22 Set Up CTC Computer to Connect to the ONS 15327 2-8
NTP-B23 Log into the ONS 15327 GUI 2-22

CHAPTER 3 **Turn Up Node** 3-1

NTP-B24 Verify Card Installation 3-2
NTP-B30 Create Users and Assign Security 3-3
NTP-B25 Set Up Name, Date, Time, and Contact Information 3-5
NTP-B169 Set Up CTC Network Access 3-7
NTP-B27 Set Up the ONS 15327 for Firewall Access 3-13
NTP-B28 Set Up Timing 3-16
NTP-B170 Create Optical Protection Groups 3-20
NTP-B171 Set Up SNMP 3-21
NTP-B34 Create Ethernet RMON Alarm Thresholds 3-23

CHAPTER 4 **Turn Up Network** 4-1

NTP-B35 Verify Node Turn Up 4-2
NTP-B124 Provision a Point-to-Point Network 4-3
NTP-B173 Point-to-Point Network Acceptance Test 4-6
NTP-B38 Provision a Linear ADM Network 4-10
NTP-B174 Linear ADM Network Acceptance Test 4-11
NTP-B40 Provision BLSR Nodes 4-13

NTP-B126 Create a BLSR 4-14
NTP-B175 BLSR Acceptance Test 4-16
NTP-B44 Provision UPSR Nodes 4-22
NTP-B177 UPSR Acceptance Test 4-23
NTP-B46 Subtend a UPSR from a BLSR 4-25
NTP-B47 Subtend a BLSR from a UPSR 4-27
NTP-B48 Subtend a BLSR from a BLSR 4-27

CHAPTER 5 Create Circuits and VT Tunnels 5-1

NTP-B127 Verify Network Turn Up 5-3
NTP-B181 Create an Automatically Routed DS-1 Circuit 5-5
NTP-B182 Create a Manually Routed DS-1 Circuit 5-9
NTP-B183 Create a Unidirectional DS-1 Circuit with Multiple Drops 5-11
NTP-B184 Create an Automatically Routed DS-3 Circuit 5-16
NTP-B185 Create a Manually Routed DS-3 Circuit 5-20
NTP-B186 Create a Unidirectional DS-3 Circuit with Multiple Drops 5-22
NTP-B133 Create an Automatically Routed VT Tunnel 5-28
NTP-B134 Create a Manually Routed VT Tunnel 5-30
NTP-B135 Test Electrical Circuits 5-33
NTP-B188 Create an Automatically Routed Optical Circuit 5-35
NTP-B189 Create a Manually Routed Optical Circuit 5-38
NTP-B190 Create a Unidirectional Optical Circuit with Multiple Drops 5-41
NTP-B62 Test Optical Circuits 5-46
NTP-B191 Create an E-Series EtherSwitch Circuit (Multicard or Single-Card Mode) 5-48
NTP-B192 Create a Circuit for an E-Series Card in Port-Mapped Mode 5-50
NTP-B142 Create an E-Series Shared Packet Ring Ethernet Circuit 5-52
NTP-B143 Create an E-Series Hub and Spoke Ethernet Configuration 5-55
NTP-B144 Create an E-Series Single-Card EtherSwitch Manual Cross-Connect 5-57
NTP-B145 Create an E-Series Multicard EtherSwitch Manual Cross-Connect 5-60
NTP-B146 Test E-Series Circuits 5-67
NTP-B147 Create a G-Series Circuit 5-68
NTP-B148 Create a Manual Cross-Connect for a G-Series or an E-Series in Port-Mapped Mode 5-70
NTP-B149 Test G-Series Circuits 5-73
NTP-B194 Create Overhead Circuits 5-74

CHAPTER 6 Manage Alarms 6-1

NTP-B195 Document Existing Provisioning 6-2
NTP-B196 View Alarms, History, Events, and Conditions 6-5
NTP-B68 Delete Cleared Alarms from Display 6-12
NTP-B69 View Alarm-Affected Circuits 6-13
NTP-B70 Create, Download, and Assign Alarm Severity Profiles 6-15
NTP-B168 Enable, Modify, or Disable Alarm Severity Filtering 6-25

NTP-B72 Suppress and Discontinue Alarm Suppression 6-29
NTP-B32 Provision External Alarms and Controls on the XTC 6-32

CHAPTER 7 Monitor Performance 7-1

NTP-B73 Enable Performance Monitoring 7-2
NTP-B195 Monitor Electrical or Optical Performance 7-6
NTP-B198 Monitor Ethernet Performance 7-15

CHAPTER 8 Manage Circuits 8-1

NTP-B199 Locate and View Circuits 8-3
NTP-B151 Modify Circuit Characteristics 8-7
NTP-B416 Convert a CTC Circuit to TL1 Cross-Connects 8-11
NTP-B417 Upgrade TL1 Cross-Connects to CTC Circuits 8-13
NTP-B152 Delete Circuits 8-13
NTP-B78 Create a Monitor Circuit 8-14
NTP-B79 Create a J1 Path Trace 8-15

CHAPTER 9 Change Port Settings 9-1

NTP-B88 Modify Line Settings and PM Parameter Thresholds for Electrical Ports 9-1
NTP-B89 Modify Line Settings and PM Parameter Thresholds for Optical Ports 9-9

CHAPTER 10 Change Node Settings 10-1

NTP-B81 Change Node Management Information 10-2
NTP-B201 Change CTC Network Access 10-4
NTP-B202 Customize the CTC Network View 10-7
NTP-B203 Modify or Delete 1+1 Card Protection Settings 10-12
NTP-B204 Delete a SONET DCC Termination 10-14
NTP-B85 Change Node Timing 10-15
NTP-B205 Modify Users and Change Security 10-17
NTP-B87 Change SNMP Settings 10-23

CHAPTER 11 Upgrade Cards and Spans 11-1

NTP-B229 Upgrade the XTC-14 Card to XTC-28 Card 11-1
NTP-B94 Upgrade Optical Spans Automatically 11-3
NTP-B95 Upgrade Optical Spans Manually 11-5

CHAPTER 12 Convert Network Configurations 12-1

NTP-B154 Convert a Point-to-Point to a Linear ADM 12-1
NTP-B155 Convert a Point-to-Point or a Linear ADM to a Two-Fiber BLSR 12-3
NTP-B156 Convert a Point-to-Point or Linear ADM to a UPSR 12-6
NTP-B210 Convert a USPR to a Two-Fiber BLSR 12-6
NTP-B159 Modify a BLSR 12-8

CHAPTER 13 Add and Remove Nodes 13-1

NTP-B12 Add a BLSR Node 13-2

NTP-B213 Remove a BLSR Node 13-9

NTP-B105 Add a UPSR Node 13-13

NTP-B106 Remove a UPSR Node 13-15

CHAPTER 14 Maintain the Node 14-1

NTP-B107 Inspect and Maintain the Air Filter 14-2

NTP-B108 Back Up the Database 14-6

NTP-B109 Restore the Database 14-8

NTP-B163 Restore the Node to Factory Configuration 14-10

NTP-B214 Offload the Security Audit Trail Log 14-15

NTP-B110 Inhibit Protection Switching 14-16

NTP-B111 Revert to an Earlier Software Load 14-19

NTP-B112 Clean Fiber Connectors 14-20

NTP-B113 Reset the XTC Using CTC 14-23

NTP-B215 View G1000-2 Ethernet Maintenance Information 14-24

NTP-B228 View E10/100-4 Ethernet Maintenance Information 14-25

NTP-B225 Switch the Node Timing Reference 14-27

CHAPTER 15 Power Down the Node 15-1

NTP-B114 Power Down the ONS 15327 15-1

appendix A-1 CTC Information and Shortcuts A-1

appendix B-1 Shelf Assembly Specifications B-1

appendix C-1 Network Element Defaults C-1

NTP-B164 Edit Network Element Defaults C-2

NTP-B165 Import Network Element Defaults C-3

NTP-B166 Export Network Element Defaults C-4

appendix D-1 Alternate Installation Procedures D-1

NTP-B223 Install the Fiber-Optic Cable Storage Drawer D-2

NTP-B224 Route Cables Through the Fiber-Optic Cable Storage Drawer D-2

NTP-B222 Connect Office Power to the ONS 15327 Shelf (Terminal-Lug Power Connector) D-4

TASKS

CHAPTER 1 **Install Hardware** 1-1

DLP-B1 Unpack and Verify the Shelf Assembly 1-4

DLP-B2 Inspect the Shelf Assembly 1-5

DLP-B3 Reverse the Mounting Bracket to Fit a 19-inch Rack 1-6

DLP-B5 Mount the ONS 15327 in a Rack 1-8

DLP-B7 Mount Multiple Shelf Assemblies in a Rack 1-8

DLP-B329 Install the Tie-Down Bar 1-9

DLP-B16 Connect the Office Ground to the ONS 15327 1-13

DLP-B17 Connect Office Power to the ONS 15327 Shelf (Screw-Lock Power Connector) 1-14

DLP-B18 Turn On and Verify Office Power 1-19

DLP-B30 Install Ferrites on Power Cabling 1-20

DLP-B4 Install SFP Connectors on G1000-2 Cards 1-24

DLP-B6 Remove SFP Connectors from G1000-2 Cards 1-25

DLP-B320 Delete a Card 1-26

DLP-B247 Change an Optical Card 1-27

DLP-B321 Install External Alarm Cables 1-29

DLP-B322 Install Timing Cables 1-30

DLP-B323 Install the Serial Cable for TL1 Craft Interface 1-32

DLP-B324 Install DS-1 Champ Cables on a MIC 1-34

DLP-B325 Install Coaxial Cable With BNC Connectors 1-38

DLP-B326 Route Electrical Cables 1-39

DLP-B327 Install Fiber-Optic Cables on the LGX Interface 1-42

DLP-B42 Install Fiber-Optic Cables on OC-N Cards 1-42

DLP-B43 Install Fiber-Optic Cables for UPSR Configurations 1-43

DLP-B44 Install Fiber-Optic Cables for BLSR Configurations 1-46

DLP-B46 Route Fiber-Optic Cables 1-47

DLP-B33 Measure Voltage 1-49

CHAPTER 2 **Connect the PC and Log into the GUI** 2-1

DLP-B47 Run the CTC Installation Wizard for Windows 2-2

DLP-B48 Run the CTC Installation Wizard for UNIX 2-5

DLP-B49 Set Up the Java Runtime Environment for UNIX 2-7

DLP-B50 Set Up a Windows PC for Craft Connection to an ONS 15327 on the Same Subnet Using Static IP Addresses 2-11

DLP-B51 Set Up a Windows PC for Craft Connection to an ONS 15327 Using DHCP 2-13

DLP-B52 Set Up a Windows PC for Craft Connection to an ONS 15327 Using Automatic Host Detection 2-15

DLP-B53 Set Up a Solaris Workstation for a Craft Connection to an ONS 15327 2-17

DLP-B55 Set Up a Computer for a Corporate LAN Connection 2-19

DLP-B56 Disable Proxy Service Using Internet Explorer (Windows) 2-20

DLP-B57 Disable Proxy Service Using Netscape (Windows and UNIX) 2-20

DLP-B58 Provision Remote Access to the ONS 15327 2-21

DLP-B59 Connect Computer to the ONS 15327 2-22

DLP-B60 Log into CTC 2-23

DLP-B61 Create Login Node Groups 2-25

DLP-B62 Add a Node to the Current Session or Login Group 2-26

CHAPTER 3 Turn Up Node 3-1

DLP-B74 Create a New User - Single Node 3-3

DLP-B75 Create a New User - Multiple Nodes 3-4

DLP-B249 Provision IP Settings 3-7

DLP-B65 Create a Static Route 3-9

DLP-B250 Set Up or Change Open Shortest Path First Protocol 3-10

DLP-B251 Set Up or Change Routing Information Protocol 3-12

DLP-B67 Provision the IIOP Listener Port on the ONS 15327 3-14

DLP-B68 Provision the IIOP Listener Port on the CTC Computer 3-16

DLP-B69 Set Up External or Line Timing 3-17

DLP-B70 Set Up Internal Timing 3-19

CHAPTER 4 Turn Up Network 4-1

DLP-B253 Provision SONET DCC Terminations 4-4

DLP-B214 Change the Service State for a Port 4-5

DLP-B254 XTC Active/Standby Switch Test 4-7

DLP-B88 Optical 1+1 Protection Test 4-8

DLP-B217 BLSR Exercise Ring Test 4-18

DLP-B91 BLSR Ring Switch Test 4-19

DLP-B94 UPSR Protection Switching Test 4-25

CHAPTER 5 **Create Circuits and VT Tunnels** 5-1

DLP-B314 Assign a Name to a Port 5-14

DLP-B95 Provision a DS-1 Circuit Source and Destination 5-15

DLP-B218 Provision UPSR Selectors During Circuit Creation 5-25

DLP-B208 Provision a DS-3 Circuit Source and Destination 5-26

DLP-B96 Provision a DS-1 or DS-3 Circuit Route 5-27

DLP-B219 Provision a VT Tunnel Route 5-32

DLP-B97 Provision an Optical Circuit Source and Destination 5-44

DLP-B98 Provision an Optical Circuit Route 5-45

DLP-B99 Determine Available VLANs 5-63

DLP-B246 Provision E-Series Ethernet Card Mode 5-64

DLP-B220 Provision E-Series Ethernet Ports 5-64

DLP-B221 Provision E-Series Ethernet Ports for VLAN Membership 5-65

DLP-B222 Provision G-Series Ethernet Ports 5-72

DLP-B313 Create a DCC Tunnel 5-75

DLP-B212 Create a User Data Channel 5-76

CHAPTER 6 **Manage Alarms** 6-1

DLP-B138 Print CTC Data 6-2

DLP-B139 Export CTC Data 6-3

DLP-B110 View Alarm History 6-7

DLP-B111 Changing the Maximum Number of Session Entries for Alarm History 6-9

DLP-B112 Display Alarms and Conditions Using Time Zone 6-10

DLP-B113 Synchronize Alarms 6-10

DLP-B114 View Conditions 6-11

DLP-B115 Create Alarm Severity Profiles 6-16

DLP-B223 Download an Alarm Severity Profile 6-19

DLP-B116 Apply Alarm Profiles to Ports 6-20

DLP-B117 Apply Alarm Profiles to Cards and Nodes 6-23

DLP-B118 Delete Alarm Severity Profiles 6-24

DLP-B225 Enable Alarm Filtering 6-26

DLP-B226 Modify Alarm and Condition Filtering Parameters 6-27

DLP-B227 Disable Alarm Filtering 6-29

DLP-B119 Suppress Alarm Reporting 6-30

DLP-B120 Discontinue Alarm Suppression 6-31

CHAPTER 7 **Monitor Performance** 7-1

DLP-B121 Enable Pointer Justification Count Performance Monitoring 7-2

DLP-B122 Enable Intermediate-Path Performance Monitoring 7-4

DLP-B123 View Electrical PM Parameters 7-7

DLP-B261 Refresh PM Counts for a Different Port 7-8

DLP-B124 Refresh Electrical or Optical PM Counts at Fifteen-Minute Intervals 7-8

DLP-B318 Refresh Electrical or Optical PM Counts at One-Day Intervals 7-9

DLP-B126 Monitor Near-End PM Counts 7-10

DLP-B127 Monitor Far-End PM Counts 7-10

DLP-B129 Reset Current PM Counts 7-11

DLP-B130 Clear Selected PM Counts 7-11

DLP-B260 Set Auto-Refresh Interval for Displayed PM Counts 7-12

DLP-B317 View Optical OC-N PM Parameters 7-13

DLP-B319 Monitor PM Counts for Selected Signal Types 7-14

DLP-B256 View Ethernet Statistics PM Parameters 7-16

DLP-B257 View Ethernet Utilization PM Parameters 7-17

DLP-B259 Refresh Ethernet PM Counts at a Different Time Interval 7-18

DLP-B258 View Ethernet History PM Parameters 7-18

CHAPTER 8 **Manage Circuits** 8-1

DLP-B262 Filter the Display of Circuits 8-4

DLP-B131 Search for Circuits 8-5

DLP-B229 View Circuits on a Span 8-6

DLP-B230 Change a Circuit State 8-7

DLP-B231 Edit a Circuit Name 8-8

DLP-B232 Change Active and Standby Span Color 8-9

DLP-B233 Edit UPSR Circuit Path Selectors 8-10

DLP-B264 Provision Path Trace on Circuit Source and Destination Ports 8-16

DLP-B137 Provision Path Trace on OC-N Ports 8-19

CHAPTER 9 **Change Port Settings** 9-1

DLP-B165 Change Line and Threshold Settings for the DS-1 Ports 9-2

DLP-B166 Change Line and Threshold Settings for the DS-3 Ports 9-6

DLP-B170 Change Line Settings for OC-N Cards 9-9

DLP-B171 Change SONET Thresholds Settings for OC-N Cards 9-11

DLP-B172 Change an Optical Port to SDH 9-14

CHAPTER 10 Change Node Settings 10-1

DLP-B140 Change the Node Name, Date, Time, and Contact Information 10-2

DLP-B265 Change the Login Legal Disclaimer 10-3

DLP-B266 Change IP Settings 10-5

DLP-B142 Modify a Static Route 10-6

DLP-B143 Delete a Static Route 10-6

DLP-B144 Disable the Open Shortest Path First Protocol 10-7

DLP-B145 Change the Network View Background Color 10-8

DLP-B267 Change the Default Network View Background Map 10-8

DLP-B268 Apply a Custom Network View Background Map 10-9

DLP-B148 Create Domain Icons 10-10

DLP-B149 Manage Domain Icons 10-10

DLP-B269 Enable Dialog Box Do-Not-Display Option 10-11

DLP-B154 Modify a 1+1 Protection Group 10-13

DLP-B155 Delete a Protection Group 10-14

DLP-B157 Change the Node Timing Source 10-15

DLP-B271 Change Node Security Policy - Single Node 10-17

DLP-B272 Change Node Security Policy - Multiple Nodes 10-18

DLP-B158 Change User and Security Settings - Single Node 10-19

DLP-B160 Change User and Security Settings - Multiple Nodes 10-20

DLP-B315 Log Out a User - Single Node 10-20

DLP-B316 Log Out a User - Multiple Nodes 10-21

DLP-B159 Delete User - Single Node 10-22

DLP-B161 Delete User - Multiple Nodes 10-22

DLP-B273 Modify SNMP Trap Destination 10-24

DLP-B163 Delete SNMP Trap Destinations 10-25

DLP-B164 Delete Ethernet RMON Alarm Thresholds 10-25

CHAPTER 11 Upgrade Cards and Spans 11-1

DLP-B293 Perform a Manual Span Upgrade on a Two-Fiber BLSR 11-6

DLP-B295 Perform a Manual Span Upgrade on a UPSR 11-8

DLP-B296 Perform a Manual Span Upgrade on a 1+1 Protection Group 11-9

DLP-B297 Perform a Manual Span Upgrade on an Unprotected Span 11-11

CHAPTER 12 Convert Network Configurations 12-1

DLP-B298 Check the Network for Alarms and Conditions 12-3

DLP-B189 Verify that a 1+1 Working Slot is Active 12-5

DLP-B301 Initiate a BLSR Manual Ring Switch 12-9

DLP-B241 Clear a BLSR Manual Ring Switch 12-10

CHAPTER 13 **Add and Remove Nodes 13-1**

DLP-B302 Check BLSR or UPSR Alarms and Conditions 13-5

DLP-B242 Create a BLSR on a Single Node 13-6

DLP-B303 Initiate a BLSR Force Ring Switch 13-6

DLP-B194 Clear a BLSR Force Ring Switch 13-8

DLP-B304 Verify BLSR Pass-Through Circuits 13-11

DLP-B195 Verify Timing in a Reduced Ring 13-12

DLP-B196 Delete a BLSR from a Single Node 13-12

DLP-B197 Initiate a UPSR Force Switch 13-16

DLP-B198 Clear a UPSR Switch 13-17

CHAPTER 14 **Maintain the Node 14-1**

DLP-B199 Inspect, Clean, and Replace the Reusable Air Filter 14-2

DLP-B200 Inspect and Replace the Disposable Air Filter 14-4

DLP-B244 Use the Reinitialization Tool to Clear the Database and Upload Software (Windows) 14-11

DLP-B245 Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX) 14-13

DLP-B201 Apply a Lock On 14-16

DLP-B202 Apply a Lock Out 14-17

DLP-B203 Clear a Lock On or Lock Out 14-18

DLP-B204 Scope and Clean Fiber Connectors and Adapters with Alcohol and Dry Wipes 14-21

DLP-B205 Clean Fiber Connectors with CLETOP 14-21

DLP-B206 Clean the Fiber Adapters 14-22

DLP-B306 View Loopback Status 14-24

DLP-B307 View Ethernet Bandwidth Usage 14-25

DLP-B309 View Ethernet MAC Address Table 14-26

DLP-B310 View Ethernet Trunk Utilization 14-26

DLP-B330 Manual or Force Switch the Node Timing Reference 14-27

DLP-B331 Clear a Manual or Force Switched Node Timing Reference 14-28

CHAPTER 15 **Power Down the Node 15-1**

About this Guide

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

This section provides the following information:

- Document Objectives
- Audience
- Document Organization
- Related Documentation
- Document Conventions
- Where to Find Safety and Warning Information
- Obtaining Documentation
- Obtaining Technical Assistance
- Obtaining Additional Publications and Information

Document Objectives

This procedure guide explains how to install, turn up, provision, and maintain a Cisco ONS 15327node and network. Use this document in conjunction with the appropriate publications listed in the Related Documentation section.

Audience

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

Document Organization

This guide provides procedures for installation, turn up, provisioning and acceptance of ONS 15327 nodes and ONS 15327 designed networks. It is organized in a Cisco recommended work flow sequence for new installations, in addition to allowing easy access to procedures and tasks associated with adds, moves, and changes for existing installations.

Verification procedures are provided, where necessary, to allow contract vendors to complete the physical installation and then turn the site over to craft personnel for verification, provisioning, turn up and acceptance. The front matter of the book is present in the following sequence:

1. Title Page
2. Table of Contents
3. List of Figures
4. List of Tables
5. List of Procedures
6. List of Tasks

The information in the book follows a task oriented hierarchy using the elements described below.

Chapter (Director Level)

The guide is divided into logical work groups (chapters) that serve as director entry into the procedures. For example, if you are arriving on site after a contractor has installed the shelf hardware, proceed to Chapter 1, "Install Hardware" and begin verifying installation and installing cards. You may proceed sequentially (recommended), or locate the work you want to perform from the list of procedures on the first page of every chapter (or turn to the front matter or index).

Non-Trouble Procedure (NTP)

Each NTP is a list of steps designed to accomplish a specific procedure. Follow the steps until the procedure is complete. If you need more detailed instructions, refer to the Detailed Level Procedure (DLP) specified in the procedure steps.

Note Throughout this guide, NTPs are referred to as "procedures" and DLPs are termed "tasks." Every reference to a procedure includes its NTP number, and every reference to a task includes its DLP number.

Detailed Level Procedure (DLP)

The DLP (task) supplies additional task details to support the NTP. The DLP lists numbered steps that lead you through completion of a task. Some steps require that equipment indications be checked for verification. When the proper response is not obtained, a trouble clearing reference is provided.

Related Documentation

Use the *Cisco ONS 15327 Procedure Guide, Release 3.4* in conjunction with the following publications:

- *Cisco ONS 15327 Troubleshooting Guide, Release 3.4*
  Provides alarm descriptions and troubleshooting procedures, hardware replacement instructions, and general troubleshooting information
- *Cisco ONS 15327 Reference Manual, Release 3.4*
  Provides card specifications and reference information regarding ONS 15327 features and functions.
- *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide, Release 3.4*
  Provides a comprehensive list of TL1 commands for the ONS 15327 and the ONS 15454
- *Release Notes for Cisco ONS 15327 Release 3.4, Release 3.4*
  Provides caveats, closed issues, and new feature information

Document Conventions

This publication uses the following conventions:

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

Warning **Means *danger*. The user is in a situation that could cause bodily injury. Before working on any equipment, be aware of the hazards involved with electrical circuitry and optical lasers and be familiar with standard practices for preventing accidents.**

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

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

Where to Find Safety and Warning Information

For safety and warning information, refer to the *Cisco ONS 15327 Installation Handbook* that accompanied the product. This publication describes the international agency compliance and safety information for the Cisco ONS 15327. It also includes translations of the safety warnings that appear in the ONS 15327 documentation.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

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

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

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

Documentation CD-ROM

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

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

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

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

Documentation Feedback

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

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

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

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

Technical Assistance Center

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

We categorize Cisco TAC inquiries according to urgency:

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

Cisco TAC Website

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

http://www.cisco.com/tac

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

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

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

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

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

Cisco TAC Escalation Center

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

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

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

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

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

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

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

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

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

CHAPTER 1

Install Hardware

This chapter provides procedures for installing the Cisco ONS 15327 shelf, cards, and fiber-optic cable. To view a summary of the tools and equipment required for installation, see the "Required Tools and Equipment" section on page 1-2.

Before You Begin

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-B1 Unpack and Inspect the ONS 15327 Shelf Assembly, page 1-4—Complete this procedure before continuing with the "NTP-B2 Install the Shelf Assembly" procedure on page 1-5.
2. NTP-B2 Install the Shelf Assembly, page 1-5—Complete this procedure to install the shelf assembly in a rack before continuing with the "NTP-B216 Install the Mechanical Interface Cards" procedure on page 1-11.
3. NTP-B216 Install the Mechanical Interface Cards, page 1-11—Complete this procedure to install the Mechanical Interface cards (MICs) before continuing with the "NTP-B6 Install the Power and Ground" procedure on page 1-12.
4. NTP-B6 Install the Power and Ground, page 1-12—Complete this procedure before continuing with the "NTP-B7 Install the Fan-Tray Assembly" procedure on page 1-20.
5. NTP-B7 Install the Fan-Tray Assembly, page 1-20—Complete this procedure to install the fan-tray assembly in the shelf before continuing with the "NTP-B217 Install the XTCs" procedure on page 1-21.
6. NTP-B217 Install the XTCs, page 1-21—Complete this procedure to install the Cross-Connect Timing and Control (XTC) cards.
7. NTP-B218 Install the Optical and Ethernet Cards, page 1-23—As needed, complete this procedure to install optical and Ethernet cards.
8. NTP-B219 Remove and Replace a Card, page 1-26—As needed, complete this procedure to remove and replace an ONS 15327 card.
9. NTP-B115 Preprovision a Slot, page 1-28—As needed, complete this procedure to preprovision any empty card slot with a card that will be installed later.
10. NTP-B8 Install Wires to Alarm, Timing, LAN, and Craft Pin Connections, page 1-28—Complete this procedure to install cables for alarms, timing, and LAN connections.
11. NTP-B220 Install the Electrical Cables, page 1-33—Complete this procedure to connect and route cables that will carry electrical traffic.

12. NTP-B221 Install Optical Cables, page 1-40—Complete this procedure to connect and route cables that will carry optical traffic.
13. NTP-B13 Perform the Shelf Installation Acceptance Test, page 1-48—Complete this procedure to determine if you have correctly completed all other procedures in the chapter.

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

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

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

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

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

Required Tools and Equipment

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

Included Materials

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

- #12-24 x 1/2 pan head Phillips mounting screws (4)
- #10-32 x 3/8 pan head Phillips power lug screws (2)
- #12 AWG dual hole 5/8 in. spaced grounding lug
- Electrostatic discharge (ESD) wrist strap with 1.8 m (6 ft.) coil cable
- Screw-lock power connector
- Terminal-lug power connector
- Terminal lugs (4)
- Terminal lug screws (4)
- Straight DS-1 cable

- Tie-down bar (optional) (15327-TIE-BAR-19 for a 19-inch rack or 15327-TIE-BAR-23 for a 23-inch rack)
- Cable storage tray and screws (4) (optional)

User-Supplied Materials

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

- Equipment rack (22 inches total width for a 19-inch rack; 26 inches total width for a 23-inch rack)
- Fuse panel
- Copper power cable (from fuse and alarm panel to assembly), #12-16 AWG

  The National Electrical Code recommends #12-14 AWG power cable
- Ground cable, #12 AWG stranded (minimum)
- Alarm cable, CAT-5 terminated with RJ-45 for all alarm connections
- Building Integrated Timing Supply (BITS) clock cable, 100-ohm #22 or #24 (0.51 mm^2 or 0.64 mm^2), twisted-pair, T1-type, shielded AWG wire
- Serial cable, DB-9 connectors
- Single-mode SC fiber jumpers with UPC polish (55 dB or better) for OC12 and OC-48 cards and fiber jumpers with LC connectors for the OC-3 card
- Shielded ABAM cable terminated with Champ connectors for DS-1 ports with #22 or #24 AWG ground wire (optional)
- Shielded coaxial cable terminated with BNC connectors for DS-3 ports
- Tie wraps and/or lacing cord
- Labels

Tools Needed

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

Test Equipment

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

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

NTP-B1 Unpack and Inspect the ONS 15327 Shelf Assembly

Purpose	This procedure describes how to unpack the ONS 15327 and verify the contents.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Complete the "DLP-B1 Unpack and Verify the Shelf Assembly" task on page 1-4.

Step 2 Complete the "DLP-B2 Inspect the Shelf Assembly" task on page 1-5.

Step 3 Continue with the "NTP-B2 Install the Shelf Assembly" procedure on page 1-5.

Stop. You have completed this procedure.

DLP-B1 Unpack and Verify the Shelf Assembly

Purpose	This task removes the shelf assembly from the package.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 When you receive the ONS 15327 system equipment at the installation site, open the top of the box. The Cisco Systems logo designates the top of the box.

Step 2 Remove the foam inserts from the box. The box contains the ONS 15327 shelf (wrapped in plastic) and a smaller box containing items needed for installation.

Step 3 To remove the shelf, grasp both sides of the shelf and slowly lift it out of the box.

Step 4 Open the smaller box containing installation materials, and verify that you have all items listed in the "Included Materials" section on page 1-2.

Note The fan-tray assembly is shipped separately.

Step 5 Return to your originating procedure (NTP).

DLP-B2 Inspect the Shelf Assembly

Purpose	This task verifies that all parts of the shelf assembly are in good condition.
Tools/Equipment	None
Prerequisite Procedures	DLP-B1 Unpack and Verify the Shelf Assembly, page 1-4
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Verify the following:

- Pins are not bent or broken
- Frame is not bent

Step 2 If the pins are bent or broken, or the frame is bent, call your Cisco sales engineer for a replacement.

Step 3 Return to your originating procedure (NTP).

NTP-B2 Install the Shelf Assembly

Purpose	This procedure describes how to reverse the mounting bracket and mount shelf assemblies in a rack.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Two set screws (48-1003-XX)
Prerequisite Procedures	NTP-B1 Unpack and Inspect the ONS 15327 Shelf Assembly, page 1-4
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **To prevent the equipment from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 131°F (55°C). To prevent airflow restriction, allow at least 3 inches (7.6 cm) of clearance around the ventilation openings.**

Warning **The ONS 15327 must have 1 inch of airspace below the installed shelf assembly 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.**

Step 1 Complete the "DLP-B3 Reverse the Mounting Bracket to Fit a 19-inch Rack" task on page 1-6 if you need to convert from a 23-inch to a 19-inch rack.

Step 2 Complete the necessary rack mount task:

- DLP-B5 Mount the ONS 15327 in a Rack, page 1-8
- DLP-B7 Mount Multiple Shelf Assemblies in a Rack, page 1-8

Step 3 As needed, complete the "DLP-B329 Install the Tie-Down Bar" task on page 1-9.

Note You can also install a cable storage drawer in the ONS 15327 rack. This drawer provides room to store up to five feet of slack and can provide a diverse cable route for redundant power feeds and cables. See the "NTP-B223 Install the Fiber-Optic Cable Storage Drawer" procedure on page D-2.

Step 4 Continue with the "NTP-B216 Install the Mechanical Interface Cards" procedure on page 1-11.

Stop. You have completed this procedure.

DLP-B3 Reverse the Mounting Bracket to Fit a 19-inch Rack

Purpose	This task installs the mounting bracket to convert a 23-inch rack to a 19-inch rack.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

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

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

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

Step 2 Flip the detached mounting bracket upside down.

Text imprinted on the mounting bracket will now also be upside down.

Step 3 Place the widest side of the mounting bracket flush against the shelf assembly (see Figure 1-1).

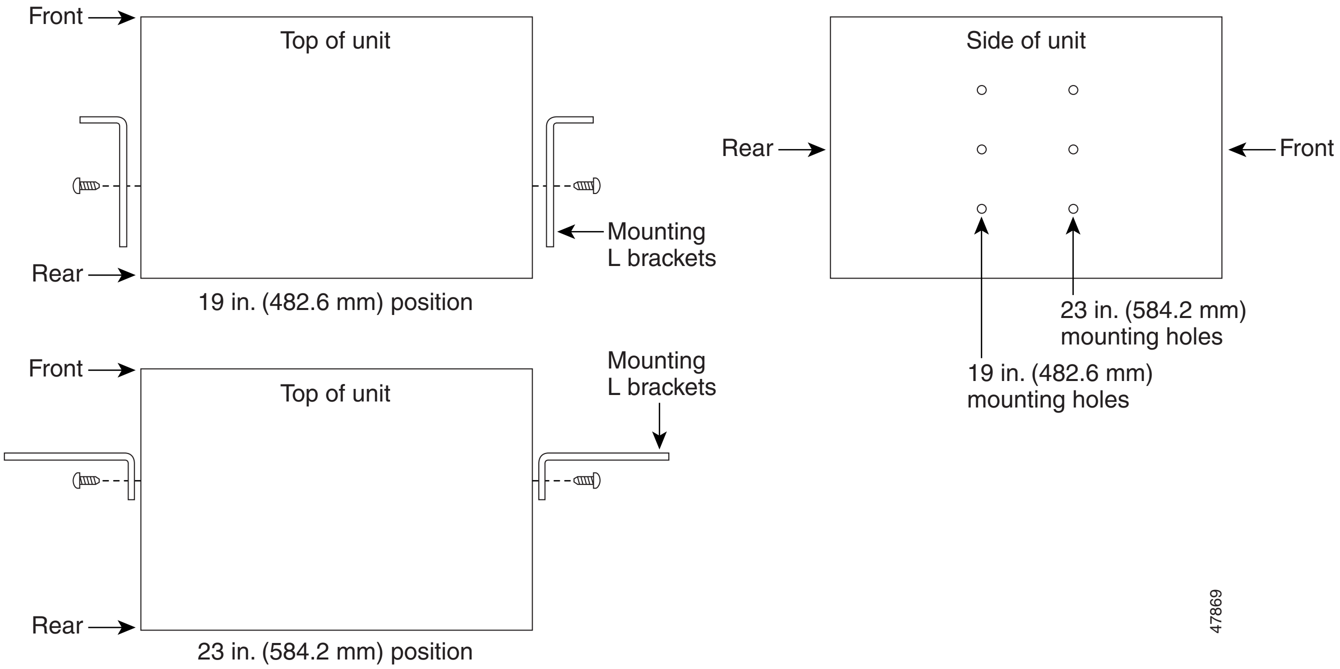
The narrow side of the mounting bracket should be towards the front of the shelf assembly. Text imprinted on the mounting bracket should be visible and upside down.

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 task for the mounting bracket on the opposite side.

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



Step 7 Return to your originating procedure (NTP).

DLP-B5 Mount the ONS 15327 in a Rack

Purpose	This task allows one person to mount the shelf assembly in a rack.
Tools/Equipment	Two sets of #12-24 mounting screws # 2 Phillips screwdriver Fuse and alarm panel, if not installed
Prerequisite Procedures	DLP-B3 Reverse the Mounting Bracket to Fit a 19-inch Rack, page 1-6, if applicable
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

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

Step 1 Verify that the proper fuse and alarm panel has been installed in the top mounting space. If a fuse and alarm panel has not been installed, you must install one according to manufacturer's instructions. A fuse panel with two 10-amp fuses per shelf is required for Power A and B feeds.

Step 2 Ensure that the shelf assembly is set for the desired rack size (either 19 or 23 inches).

Step 3 Lift the shelf assembly to the desired rack position and set it on the set screws.

Step 4 Align the screw holes on the mounting ears with the mounting holes in the rack.

Step 5 Using the Phillips screwdriver, install one mounting screw in each side of the assembly.

Step 6 When the shelf assembly is secured to the rack, install the remaining mounting screws.

Step 7 Return to your originating procedure (NTP).

DLP-B7 Mount Multiple Shelf Assemblies in a Rack

Purpose	This task installs multiple shelf assemblies in a rack.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver
Prerequisite Procedures	DLP-B3 Reverse the Mounting Bracket to Fit a 19-inch Rack, page 1-6, if applicable
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note The ONS 15327 must have one inch of air space below the installed shelf assembly to allow air flow to the fan intake. If a second ONS 15327 is installed underneath a shelf assembly, the air ramp on top of the bottom shelf assembly provides the desired space. However, if the ONS 15327 is installed above third-party equipment, you must provide a minimum spacing of one inch between the third-party shelf assembly and the bottom of the ONS 15327. The third-party equipment must not vent heat upward into the ONS 15327.

Step 1 Verify that the proper fuse and alarm panel has been installed in the top mounting space. If a fuse and alarm panel is not present, you must install one according to manufacturer instructions. A fuse panel with two 10-amp fuses per shelf is required for Power A and B feeds.

Step 2 Mount the first ONS 15327 directly below the fuse and alarm panel using the "DLP-B5 Mount the ONS 15327 in a Rack" task on page 1-8.

Note If you want to install a tie-down bar on the rack, be sure to leave 1 RU between each ONS 15327 you plan to install and the tie-down bar.

Step 3 Repeat the task with the remaining ONS 15327s (up to 12 shelves can fit in a rack).

Step 4 Return to your originating procedure (NTP).

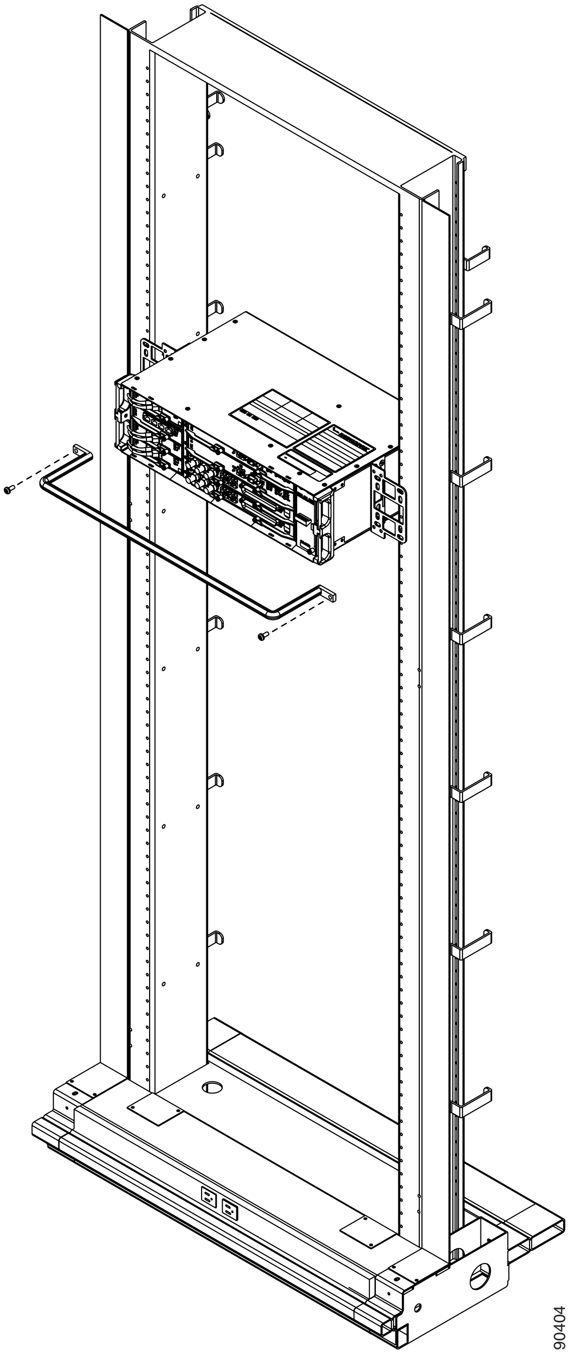
DLP-B329 Install the Tie-Down Bar

Purpose	This task installs the tie-down bar used to secure cabling on the ONS 15327. The tie-down bar can be used to provide a diverse path for redundant power feeds and cables.
Tools/Equipment	Tie-down bar Screws (4)
Prerequisite Procedures	DLP-B5 Mount the ONS 15327 in a Rack, page 1-8
Required/As Needed	As Needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Align the ends of the tie-down bar with the four screw holes located 1 RU below the ONS 15327.

Figure 1-2 shows the tie-down bar, the ONS 15327, and the rack.

Figure 1-2 Tie-Down Bar



Step 2 Install the four screws into the rack.

Step 3 Return to your originating procedure (NTP).

NTP-B216 Install the Mechanical Interface Cards

Purpose	This procedure installs the two Mechanical Interface cards (MICs) in Slots 7 and 8.
Tools/Equipment	None
Prerequisite Procedures	NTP-B2 Install the Shelf Assembly, page 1-5
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

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

Step 1 Install MIC A in Slot 8:

a. Open the card ejectors.

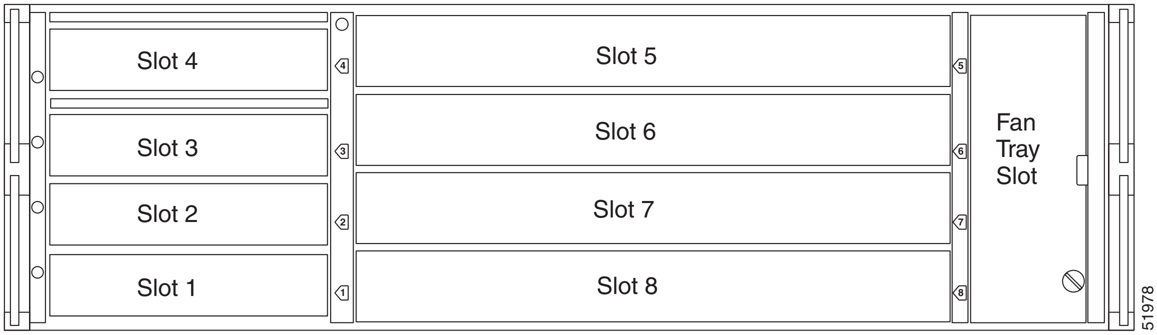
b. Slide the card along the guide rails into the slot.

c. Close the ejectors.

d. Lock the cards into place by tightening the ejector locking screws.

The slots are keyed to ensure that cards are installed in the correct slots. Figure 1-3 shows the location and number of each slot.

Figure 1-3 ONS 15327 Slot Numbering



Step 2 If you require redundant power, more than 14 DS-1s, or you are using DS-3s, install MIC B in Slot 7.

Warning **Always make sure power is disconnected before removing MICs from the ONS 15327.**

Step 3 Continue with the "NTP-B6 Install the Power and Ground" procedure on page 1-12.

Stop. You have completed this procedure.

NTP-B6 Install the Power and Ground

Purpose	This procedure describes how to install power feeds and how to ground the ONS 15327.
Tools/Equipment	Ground cable, #12 AWG stranded (minimum)
	Copper power cable (from fuse and alarm panel to assembly), #12-16 AWG (the National Electrical Code recommends #12-14 AWG power cable)
Prerequisite Procedures	NTP-B216 Install the Mechanical Interface Cards, page 1-11
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **Shut off the power from the power source or turn off the breakers before beginning work.**

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

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 15327 only to a DC power source that complies with the safety extra-low voltage (SELV) requirements in IEC 60950-based safety standards.**

Warning **The ONS 15327 relies on the protective devices in the building installation to protect against short circuit, overcurrent, and grounding faults. Ensure that the protective devices are properly rated to protect the system, and that they comply with national and local codes.**

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

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

Warning **If you use redundant power leads to power the ONS 15327 disconnecting one lead will not remove power from the node.**

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

Step 1 Verify that the proper fuse panel is installed (20-amp fuse per shelf minimum). If not, install one according to manufacturer's instructions.

Step 2 Ensure that the mechanical interface cards (MICs) are installed. See the "NTP-B216 Install the Mechanical Interface Cards" procedure on page 1-11 if necessary.

Step 3 Complete the "DLP-B16 Connect the Office Ground to the ONS 15327" task on page 1-13.

Step 4 Complete the "DLP-B17 Connect Office Power to the ONS 15327 Shelf (Screw-Lock Power Connector)" task on page 1-14.

Step 5 Complete the "DLP-B18 Turn On and Verify Office Power" task on page 1-19.

Step 6 Complete the "DLP-B30 Install Ferrites on Power Cabling" task on page 1-20.

Step 7 Continue with the "NTP-B7 Install the Fan-Tray Assembly" procedure on page 1-20.

Stop. You have completed this procedure.

DLP-B16 Connect the Office Ground to the ONS 15327

Purpose	This task connects ground to the ONS 15327 shelf.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Screws Power cable (from fuse and alarm panel to assembly), #10 AWG, copper conductors, 194°F [90°C]) Ground cable #6 AWG stranded Listed pressure terminal connectors such as ring and fork types; connectors must be suitable for #10 AWG copper conductors
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Verify that the office ground cable (#6 AWG stranded) is connected to the top of the rack according to local site practice.

Step 2 Attach one end of the shelf ground cable (#10 AWG) to the ground connection point located on the left-hand side panel as you face the ONS 15327.

Note When terminating a frame ground, use the kep-nut provided with the ONS 15327 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. The type of prevention the kep-nut provides for the frame ground connection is inherently provided by the terminal block for battery and battery return connections.

Step 3 Attach the other end of the shelf ground cable to the rack.

Step 4 Return to your originating procedure (NTP).

DLP-B17 Connect Office Power to the ONS 15327 Shelf (Screw-Lock Power Connector)

Purpose	This task connects power to the ONS 15327 shelf. You must install this power connector if you plan to install the right-angle DS-1 cable.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Wire wrapper Wire cutters Wire strippers Crimp tool Fuse panel Screw-lock power connector Power cable (from fuse and alarm panel to assembly), #10 AWG, copper conductors, 194°F [90°C]) Ground cable #6 AWG stranded Listed pressure terminal connectors such as ring and fork types; connectors must be suitable for #10 AWG copper conductors
Prerequisite Procedures	DLP-B16 Connect the Office Ground to the ONS 15327, page 1-13
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning **Do not apply power to the ONS 15327 until you complete all installation steps and check the continuity of the -48 VDC and return.**

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

Note You must install this power connector if you plan to install the right-angle DS-1 cable.

Note This procedure explains how to install the screw-lock power connector. To install the terminal-lug power connector also included with the ONS 15327, see the "NTP-B222 Connect Office Power to the ONS 15327 Shelf (Terminal-Lug Power Connector)" procedure on page D-4.

Note If you encounter problems with the power supply, refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 1 Connect the office power according to the fuse panel engineering specifications.

Step 2 Measure and cut the cables as needed to reach the ONS 15327 from the fuse panel.

Step 3 Dress the power according to local site practice.

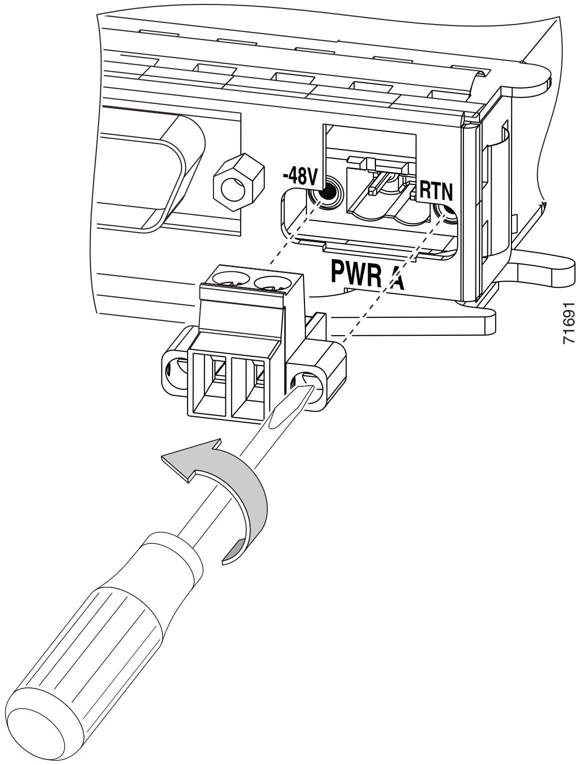
Warning **When installing the ONS 15327, the ground connection must always be made first and disconnected last.**

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

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

Step 5 If the power connector is already installed, remove it from the MIC by grasping it with your fingers and gently pulling it. If you cannot remove it easily, you can use a pair of needle nose pliers and grab it by the center of the channel. Figure 1-4 shows the MIC power connector being removed.

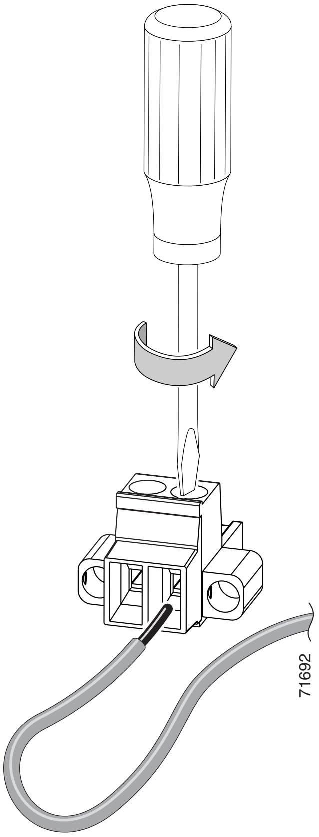
Figure 1-4 Removing the MIC Power Connector



Step 6 Remove the cable fastening screws, which are the screws on the top of the connector that become visible when the connector is removed.

Step 7 Insert the (black) return (RTN) wire into the right connector slot. Figure 1-5 shows a power cable being inserted into the MIC power connector.

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



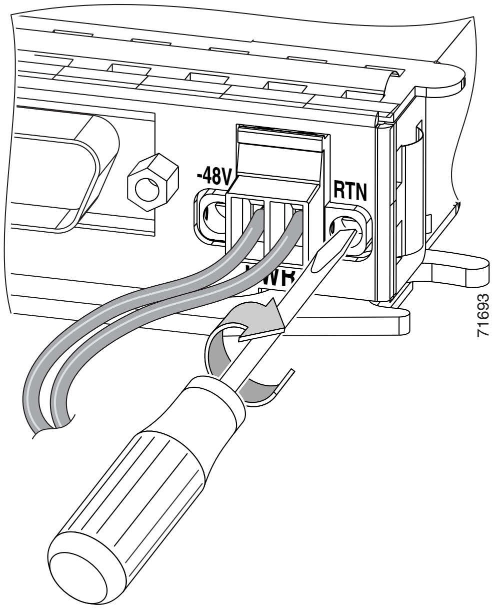
Step 8 Replace the cable fastening screw for the return (RTN) wire and tighten with a small slot-head screwdriver.

Step 9 Insert the battery (red) wire into the left (-48V) connector slot.

Step 10 Replace the cable fastening screw for the battery (-48V) wire and tighten it with the screwdriver.

Step 11 Insert the connector back into the slot on the MIC and tighten the screws with the screwdriver. Figure 1-6 shows the MIC power connector being installed.

Figure 1-6 Installing the MIC Power Connector



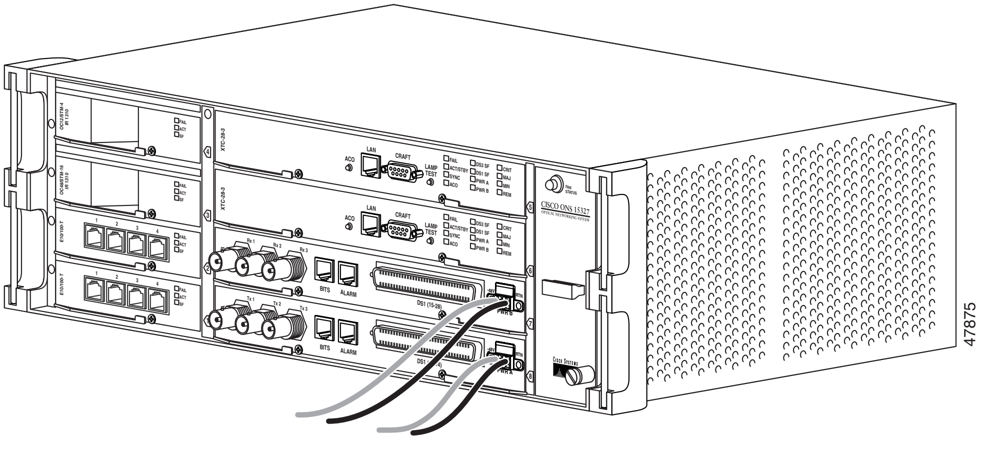
Step 12 Use a small flat-head screwdriver to open the return (RTN) terminal and insert the return lead.

Step 13 If you use redundant power feeds, repeat Steps 5 through 12 on the other MIC.

Caution In case a power cable is damaged or cut, Cisco recommends that you diversely route redundant power leads along different paths. If you installed the tie-down bar, you can run one power lead across the tie-down bar and secure it using tie-wraps or other site-specific methods. You should route the other power cable in the opposite direction.

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

Figure 1-7 Redundant Power Connections



Step 14 Return to your originating procedure (NTP).

DLP-B18 Turn On and Verify Office Power

Purpose	This task measures the power to verify correct power and returns.
Tools/Equipment	Voltmeter
Prerequisite Procedures	DLP-B16 Connect the Office Ground to the ONS 15327, page 1-13 DLP-B17 Connect Office Power to the ONS 15327 Shelf (Screw-Lock Power Connector), page 1-14
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Using a voltmeter, verify the office battery and ground at the following points on the fuse and alarm panel:

a. To verify the power, place the black test lead of the voltmeter to the frame ground. Place the red test lead on the A-side connection and verify that it is between -42 VDC and -57 VDC. Place the red test lead on the B-side connection and verify that it is between -42 VDC and -57 VDC.

Note The voltages -42 VDC and -57 VDC are the minimum and maximum amperages required to power the chassis.

b. To verify the ground, place the black test lead of the voltmeter to the frame ground. Place the red test lead on the A-side return ground and verify that no voltage is present. Place the red test lead on the B-side return ground and verify that no voltage is present.

Step 2 Insert a 10-amp fuse into the fuse position according to site practice.

Step 3 Using a voltmeter, verify the shelf for -48 VDC battery and ground:

a. To verify the A-side of the shelf, place the black lead of the voltmeter to the frame ground. Place the red test lead to the BAT1 (A-side battery connection) red cable. Verify it reads between -42 VDC and -57 VDC. Then place the red test lead of the voltmeter to the RET1 (A-side return ground) black cable and verify that no voltage is present.

b. To verify the B-side of the shelf, place the black test lead of the voltmeter to the frame ground. Place the red test lead to the BAT2 (B-side battery connection) red cable. Verify it reads between -42 VDC and -57 VDC. Then place the red test lead of the voltmeter to the RET2 (B-side return ground) black cable and verify that no voltage is present.

Step 4 Return to your originating procedure (NTP).

DLP-B30 Install Ferrites on Power Cabling

Purpose	This task installs third-party ferrites on power cables to dampen electromagnetic interference (EMI) from the ONS 15327.
Tools/Equipment	Voltmeter Block ferrite (Fair Rite 0443164151) for each pair of cables
Prerequisite Procedures	DLP-B16 Connect the Office Ground to the ONS 15327, page 1-13 DLP-B17 Connect Office Power to the ONS 15327 Shelf (Screw-Lock Power Connector), page 1-14
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Note 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.

Step 1 Wrap the cables once around and through the block ferrites.

Step 2 Place the block ferrite within 5 to 6 inches of the power terminals.

Step 3 Return to your originating procedure (NTP).

NTP-B7 Install the Fan-Tray Assembly

Purpose	This procedure installs the fan-tray assembly.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver
Prerequisite Procedures	NTP-B2 Install the Shelf Assembly, page 1-5
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Caution Do not operate an ONS 15327 without a fan-tray air filter. A fan-tray air filter is mandatory.

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

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

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

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

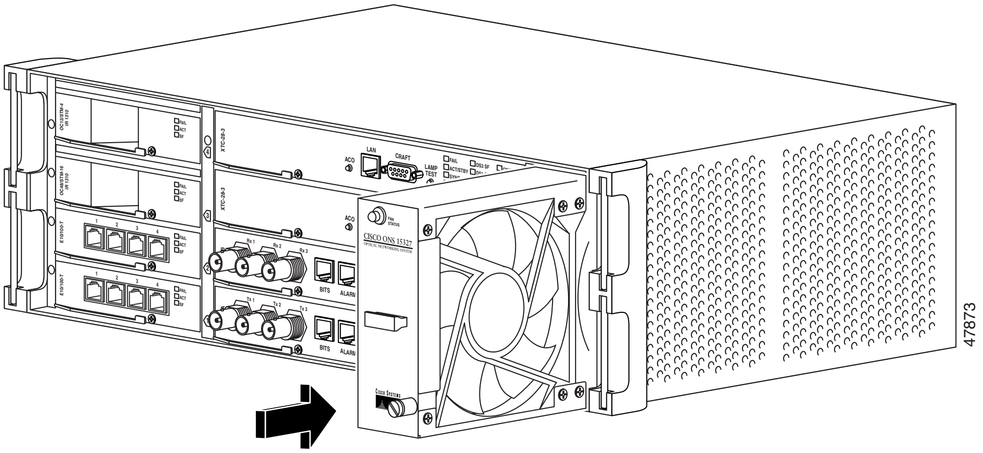
Step 3 Secure the fan-tray assembly into the slot using the attached fastening screw.

Step 4 After power is supplied, confirm that the FAN STATUS LED on the front of the fan-tray assembly is illuminated. This indicates that the fan-tray assembly is operating.

The FAN STATUS LED illuminates only when an XTC card is installed.

Figure 1-8 shows the location of the fan-tray assembly.

Figure 1-8 Installing the Fan-Tray Assembly



Step 5 Continue with the "NTP-B217 Install the XTCs" procedure on page 1-21.

Stop. You have completed this procedure.

NTP-B217 Install the XTCs

Purpose	This procedure installs the Cross-Connect Timing and Control (XTC) cards in Slots 5 and 6.
Tools/Equipment	None
Prerequisite Procedures	NTP-B7 Install the Fan-Tray Assembly, page 1-20 NTP-B216 Install the Mechanical Interface Cards, page 1-11
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Retrieve or higher

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

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

Step 1 Install an XTC card in Slot 6 (Figure 1-9):

a. Open the card ejectors.

b. Slide the card along the guide rails into the slot.

c. Close the ejectors.

d. Lock the cards into place by tightening the ejector locking screws.

Slot 6 is the working XTC card slot.

Step 2 Verify that the red FAIL LED blinks for approximately 30 seconds.

Note Older versions of the XTC card may have an amber FAIL LED.

Step 3 Verify that all LEDs blink once and turn off.

Step 4 After approximately 5 minutes, verify the ACT/STBY LED is green (active).

Step 5 Install the second XTC card in Slot 5.

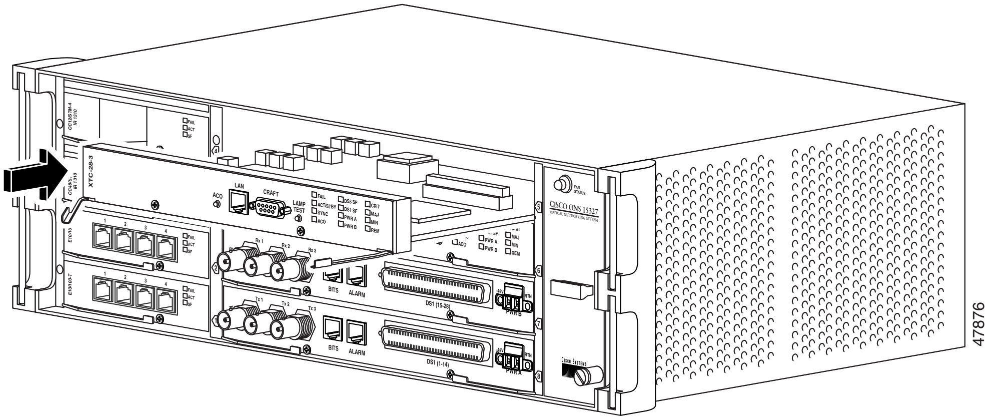
Slot 5 is the protect XTC slot.

Step 6 After the LED boot sequence (Steps 3 and 4), verify that the ACT/STBY LED is amber. The amber LED indicates that the second XTC card is the standby XTC.

Step 7 Press the LAMP TEST button on the faceplate of each XTC and verify that all LEDs illuminate while you press the button.

Step 8 When you log into CTC, verify that the card appears in the correct slot on the node view screen and that the card is white on the CTC node view screen.

Figure 1-9 Installing an XTC (XTC 28-3)



Step 9 Continue with the "NTP-B218 Install the Optical and Ethernet Cards" procedure on page 1-23.

Stop. You have completed this procedure.

NTP-B218 Install the Optical and Ethernet Cards

Purpose	This procedure installs the optical cards (OC-3, OC-12, and OC-48) and Ethernet cards (E10/100-4, G1000-2) in Slots 1 through 4.
Tools/Equipment	None
Prerequisite Procedures	NTP-B7 Install the Fan-Tray Assembly, page 1-20 NTP-B217 Install the XTCs, page 1-21
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Warning **Install blank faceplates into empty card slots. Blank faceplates serve three functions: They prevent exposure to hazardous voltages and currents inside the ONS 15327 chassis, they eliminate electromagnetic interference (EMI) that might disrupt other equipment, and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards and faceplates are in place.**

Step 1 Install an Ethernet or optical card in Slots 1, 2, 3, or 4 (Figure 1-10):

a. Open the card ejectors.

b. Slide the card along the guide rails into the slot.

c. Close the ejectors.

d. Lock the cards into place by tightening the ejector locking screws.

Step 2 Verify that the red FAIL LED illuminates for 20 to 30 seconds.

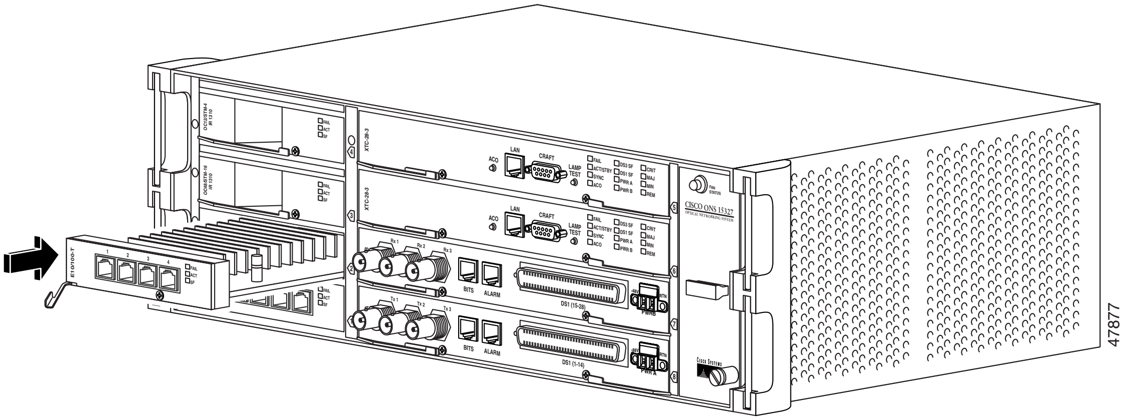
Step 3 Verify that the red FAIL LED blinks for 30 to 45 seconds.

Step 4 Verify that all LEDs blink once and turn off for 5 to 10 seconds.

Step 5 Verify the ACT LED illuminates.

Step 6 When you log into CTC, verify that the card appears in the correct slot on the CTC node view screen and appears white in node view.

Figure 1-10 Installing an Ethernet Card (E10/100-T)



Step 7 Repeat Steps 1 and 6 for each optical and Ethernet card you want to install.

Step 8 If you installed the G1000-2 card, complete the "DLP-D4 Install SFP Connectors on G1000-2 Cards" task on page 1-24.

Note If you need to remove an SFP, complete the "DLP-D6 Remove SFP Connectors from G1000-2 Cards" task on page 1-25.

Stop. You have completed this procedure.

DLP-D4 Install SFP Connectors on G1000-2 Cards

Purpose	This task installs small form-factor pluggables (SFPs) and attaches the fiber.
Tools/Equipment	Short wavelength (1000BaseSX): 15327-SFP-LC-SX Long wavelength/long haul (1000BaseLX): 15327-SFP-LC-LX
Prerequisite Procedures	NTP-B218 Install the Optical and Ethernet Cards, page 1-23
Required/As Needed	Required if you are G1000-2 cards.
Onsite/Remote	Onsite
Security Level	None

Note SFPs are hot-swappable and can be installed or removed while the card or shelf assembly is powered and running.

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 1 Remove the SFP from its protective packaging.

Step 2 Check the label to verify that the SFP is the correct type (SX or LX) for your network.

Step 3 Verify that you are installing compatible SFPs; for example, SX to SX, LX to LX. SFPs must be matched on either end by type.

Step 4 Plug the duplex connector of the fiber into a Cisco-supported SFP connector. If the new SFP connector has a latch, close the latch over the cable to secure it.

Step 5 Plug the cabled SFP connector into the G1000-2 card port until it clicks.

Step 6 Return to your originating procedure (NTP).

DLP-D6 Remove SFP Connectors from G1000-2 Cards

Purpose	This task removes SFPs from your Ethernet cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-D4 Install SFP Connectors on G1000-2 Cards, page 1-24
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Disconnect the network fiber cable from the SFP duplex connector. If the SFP connector has a latch securing the fiber cable, pull it upward to release the cable.

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

Step 2 Pull the fiber cable straight out of the connector.

Step 3 Unplug the SFP connector and fiber from the G1000-2 card.

Step 4 Slide the SFP out of the Gigabit Ethernet card slot.

Step 5 Return to your originating procedure (NTP).

NTP-B219 Remove and Replace a Card

Purpose	This procedure describes how to remove and replace cards in the ONS 15327 shelf.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 If you are not logged into CTC and you need to remove a card, remove the card as described in Step 3. When you log into CTC, troubleshoot the mismatched equipment (MEA) alarm with the *Cisco ONS 15327 Troubleshooting Guide*.

Step 2 If you are logged into CTC, either:

- Complete the "DLP-B320 Delete a Card" task on page 1-26 and continue with Step 3 or
- Complete the "DLP-B247 Change an Optical Card" task on page 1-27 to delete a card and replace it with a different optical card while maintaining existing provisioning.

Step 3 Physically remove the card:

a. Open the card latches/ejectors.

b. Use the latches/ejectors to pull the card forward and away from the shelf.

Step 4 Insert the new card using one of the following procedures as applicable:

- NTP-B217 Install the XTCs, page 1-21
- NTP-B218 Install the Optical and Ethernet Cards, page 1-23

Stop. You have completed this procedure.

DLP-B320 Delete a Card

Purpose	This task deletes a card from CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Both
Security Level	Provisioning or higher

Step 1 On the shelf graphic, right-click the card that you want to remove and choose **Delete Card**.

You cannot delete a card if any of the following conditions apply:

- The card is one of two installed XTC cards (a default XTC protection group was created); to replace an XTC card, refer to the Replace Hardware chapter in the *Cisco ONS 15454 Troubleshooting Guide*
- The card is part of a protection group; see DLP-B155 Delete a Protection Group, page 10-14

- The card has circuits; see NTP-B152 Delete Circuits, page 8-13
- The card is part of a bidirectional line switched ring (BLSR); see NTP-B213 Remove a BLSR Node, page 13-9
- The card is being used for timing; see DLP-B157 Change the Node Timing Source, page 10-15
- The card has a SONET DCC termination; see NTP-B204 Delete a SONET DCC Termination, page 10-14

Note If you do not remove a card from the shelf after you delete it in CTC, it will reboot and reappear in CTC.

Step 2 Return to your originating procedure (NTP).

DLP-B247 Change an Optical Card

Purpose	This task describes how to change an optical card while maintaining existing provisioning, including DCCs, circuits, protection, timing, and rings. You cannot change a multiport card to a card with a smaller number of ports, and you cannot change a card to an identical type of card.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Physically removing an optical card can cause a loss of working traffic or a protection switch. See Chapter 11, "Upgrade Cards and Spans" for information on upgrading traffic to a higher speed.

Step 1 If the card the active card in a 1+1 protection group, switch traffic away from the card:

a. Log into a node on the network. If you are already logged in, go to Step b.

b. Display the CTC node (login) view.

c. Click the **Maintenance > Protection** tabs.

d. Double-click the protection group that contains the reporting card.

e. Click the active card of the selected group.

f. Click **Switch** and **Yes** in the Confirmation dialog box.

Step 2 In node view, right-click the card that you want to remove and choose **Change Card**.

Step 3 From the Change Card drop-down menu, choose the desired card type and click **OK**. A Mismatched Equipment Alarm (MEA) will appear until you replace the card.

Step 4 Physically remove the card:

a. Open the card latches/ejectors.

b. Use the latches/ejectors to pull the card forward and away from the shelf.

Step 5 Return to your originating procedure (NTP).

NTP-B115 Preprovision a Slot

Purpose	This procedure describes how to preprovision a slot in the software before physical card installation.
Tools/Equipment	None
Prerequisite Procedures	Chapter 2, "Connect the PC and Log into the GUI"
Required/As Needed	As needed
Onsite/Remote	Onsite or Remote
Security Level	Provisioning or higher

Step 1 Log into the ONS 15454. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. The node (default) view displays. If you are already logged in, continue with Step 2.

Step 2 Right-click the empty slot where you will later install a card.

Step 3 From the Add Card popup menu, choose the card type that will be installed.

Note When you preprovision a slot, the card appears purple in the CTC shelf display, rather than white when a card is physically in the slot.

Step 4 Continue with the "NTP-B221 Install Optical Cables" procedure on page 1-40.

Stop. You have completed this procedure.

NTP-B8 Install Wires to Alarm, Timing, LAN, and Craft Pin Connections

Purpose	This procedure describes how to install alarm, timing, LAN, and craft wires.
Tools/Equipment	Alarm cable, CAT-5 terminated with RJ-45 for all alarm connections #22 or #24 shielded AWG wire
Prerequisite Procedures	NTP-B2 Install the Shelf Assembly, page 1-5
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Complete the "DLP-B321 Install External Alarm Cables" task on page 1-29 as necessary.

Step 2 Complete the "DLP-B322 Install Timing Cables" task on page 1-30 as needed. Timing wires are necessary to provision external timing.

Step 3 Complete the "DLP-B323 Install the Serial Cable for TL1 Craft Interface" task on page 1-32 as needed. Craft wires are required to access TL1 using the craft interface.

Step 4 Complete the "DLP-B324 Install DS-1 Champ Cables on a MIC" task on page 1-34 as needed to carry DS-1 traffic.

Step 5 Complete the "DLP-B325 Install Coaxial Cable With BNC Connectors" task on page 1-38 as needed to carry DS-3 traffic.

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

Step 6 Continue with the "NTP-B220 Install the Electrical Cables" procedure on page 1-33.

Stop. You have completed this procedure.

DLP-B321 Install External Alarm Cables

Purpose	This task installs alarm cables on the MICs so that you can provision external (environmental) alarms and controls.
Tools/Equipment	Alarm cable, CAT-5 terminated with RJ-45 for all alarm connections
Prerequisite Procedures	NTP-B2 Install the Shelf Assembly, page 1-5
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Plug one end of the alarm cable into the ALARM port on the MIC.

Step 2 Plug the other end of the cable into the alarm-collection equipment according to local site practice.

Step 3 Repeat Steps 1 and 2 for the other MIC.

Note You can use the alarm cutoff (ACO) button to extinguish audible alarms.

Step 4 To define the six external alarm inputs and two external alarm outputs using CTC, see the "NTP-B32 Provision External Alarms and Controls on the XTC" procedure on page 6-32. Table 1-1 shows the input alarm pinouts and the corresponding alarm numbers assigned to each MIC/port. Table 1-2 shows the output alarm pinouts. Refer to these tables when connecting alarm cables to the ONS 15327. See Figure 1-11 for RJ-45 pin numbering.

Table 1-1 Alarm Input Pin Assignments

Alarm Number (MIC A)	Alarm Number (MIC B)	RJ-45 Pin Number	Function
2	1	5	Alarm 2+
		6	Alarm 2-

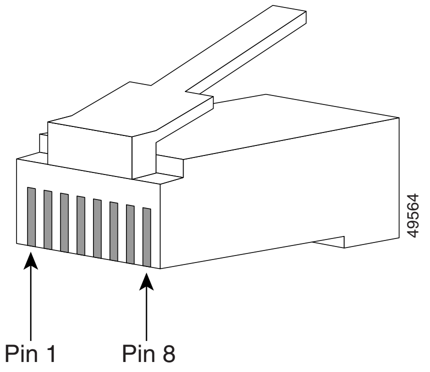
Table 1-1 Alarm Input Pin Assignments (continued)

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

Table 1-2 Alarm (External Control) Output Pin Assignments

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

Figure 1-11 Pins 1 and 8 on the RJ-45 Connector



Step 5 Return to your originating procedure (NTP).

DLP-B322 Install Timing Cables

Purpose	This task installs timing cables on the MICs so that you can provide BITS timing to the ONS 15327.
Tools/Equipment	100-ohm shielded BITS clock cable pair #22 or #24 AWG (0.51 mm² or 0.64 mm²), twisted-pair T1-type
Prerequisite Procedures	NTP-B2 Install the Shelf Assembly, page 1-5
Required/As Needed	Required if the node is using external BITS timing
Onsite/Remote	Onsite
Security Level	None

Step 1 Plug one end of the timing cable into the BITS port on the MIC.

Step 2 Plug the other end of the cable into the BITS clock according to local site practice.

Step 3 Repeat Steps 1 and 2 for the other MIC. See Table 1-3, Figure 1-12, and Figure 1-13 when connecting BITS cables to the ONS 15327.

Table 1-3 BITS Cable Pin Assignments

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

Figure 1-12 BITS In Pins on the RJ-45 Connector

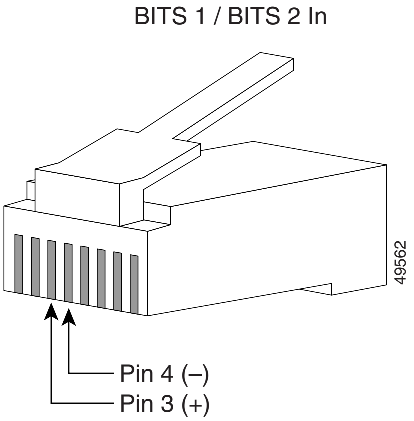


Figure 1-13 BITS Out Pins on the RJ-45 Connector

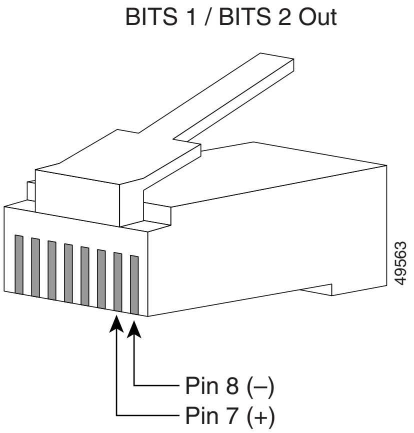


Table 1-4 External Timing Pin Assignments for BITS

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 For more detailed information about timing, refer to the *Cisco ONS 15327 Reference Manual.* To set up system timing, see the "NTP-B28 Set Up Timing" procedure on page 3-16.

Step 4 Return to your originating procedure (NTP).

DLP-B323 Install the Serial Cable for TL1 Craft Interface

Purpose	This task installs the TL1 craft interface.
Tools/Equipment	Serial cable (DB-9)
Prerequisite Procedures	NTP-B2 Install the Shelf Assembly, page 1-5
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Plug one end of the serial cable into the front of the XTC card.

Step 2 Connect the other end to the PC you want to use to access the craft.

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

Step 3 Return to your originating procedure (NTP).

NTP-B220 Install the Electrical Cables

Purpose	This procedure describes how to install the electrical DS-1 (AMP Champ) and DS-3 (coaxial) cables. To carry electrical traffic on the ONS 15327, you must install electrical cable.
Tools/Equipment	Shielded coaxial cable terminated with BNC connectors for DS-3 ports Shielded ABAM cable terminated with Champ connectors for DS-1 ports with #22 or #24 AWG ground wire (typically about two feet in length)
Prerequisite Procedures	NTP-B8 Install Wires to Alarm, Timing, LAN, and Craft Pin Connections, page 1-28
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

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

Step 1 Complete the "DLP-B324 Install DS-1 Champ Cables on a MIC" task on page 1-34 as needed.

Step 2 Complete the "DLP-B325 Install Coaxial Cable With BNC Connectors" task on page 1-38 as needed.

Step 3 Complete the "DLP-B326 Route Electrical Cables" task on page 1-39 as needed.

Step 4 Continue with the "NTP-B221 Install Optical Cables" procedure on page 1-40.

Stop. You have completed this procedure.

DLP-B324 Install DS-1 Champ Cables on a MIC

Purpose: This task installs DS-1 cables.

Tools/Equipment: One of the following DS-1 cables (either right-angle or straight):

- Right-angle DS-1 cable
  - Amphenol GCA70 03006 RSE (30 feet)
  - Amphenol GCA70 03007 RSE (50 feet)
  - Amphenol GCA70 03008 RSE (100 feet)
  - Amphenol GCA70 03009 RSE (250 feet)
  - Volex VLX979-30 (30 feet)
  - Volex VLX979-50 (50 feet)
  - Volex VLX979-100 (100 feet)
  - Volex VLX979-250 (250 feet)
- Straight DS-1 cable

Installing Champ connector DS-1 cables requires 64-pin bundled cable connectors with a 64-pin male Champ connector. You need Champ connector #552285-1 for the plug side and #1-552496-1 for the right-angle shell housing, or their functional equivalents.

Prerequisite Procedures: NTP-B8 Install Wires to Alarm, Timing, LAN, and Craft Pin Connections, page 1-28

Required/As Needed: As needed

Onsite/Remote: Onsite

Security Level: None

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

Step 1 Prepare a 56-wire cable for each DS-1 connection you will make. See Table 1-5 for the ONS 15327 Champ connector pin assignments.

Table 1-5 Pin Assignments for Champ Connector (the shaded area corresponds to the white/orange binder group)

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

Table 1-5 Pin Assignments for Champ Connector (the shaded area corresponds to the white/orange binder group) (continued)

Signal/Wire	Pin	Pin	Signal/Wire	Signal/Wire	Pin	Pin	Signal/Wire
Tx Tip 5 white/slate	5	37	Tx Ring 5 slate/white	Rx Tip 5 violet/blue	21	53	Rx Ring 5 blue/violet
Tx Tip 6 red/blue	6	38	Tx Ring 6 blue/red	Rx Tip 6 violet/orange	22	54	Rx Ring 6 orange/violet
Tx Tip 7 red/orange	7	39	Tx Ring 7 orange/red	Rx Tip 7 violet/green	23	55	Rx Ring 7 green/violet
Tx Tip 8 red/green	8	40	Tx Ring 8 green/red	Rx Tip 8 violet/brown	24	56	Rx Ring 8 brown/violet
Tx Tip 9 red/brown	9	41	Tx Ring 9 brown/red	Rx Tip 9 violet/slate	25	57	Rx Ring 9 slate/violet
Tx Tip 10 red/slate	10	42	Tx Ring 10 slate/red	Rx Tip 10 white/blue	26	58	Rx Ring 10 blue/white
Tx Tip 11 black/blue	11	43	Tx Ring 11 blue/black	Rx Tip 11 white/orange	27	59	Rx Ring 11 orange/white
Tx Tip 12 black/orange	12	44	Tx Ring 12 orange/black	Rx Tip 12 white/green	28	60	Rx Ring 12 green/white
Tx Tip 13 black/green	13	45	Tx Ring 13 green/black	Rx Tip 13 white/brown	29	61	Rx Ring 13 brown/white
Tx Tip 14 black/brown	14	46	Tx Ring 14 brown/black	Rx Tip 14 white/slate	30	62	Rx Ring 14 slate/white
Tx Spare 0+ N/A	15	47	Tx Spare0- N/A	Rx Spare0+ N/A	31	63	Rx Spare 0- N/A
Tx Spare 1+ N/A	16	48	Tx Spare1- N/A	Rx Spare1+ N/A	32	64	Rx Spare 1- N/A

Step 2 Connect the male Champ connector on the cable to the female Champ connector on the ONS 15327 MIC.

The DS-1 cable can have a straight or right-angle configuration. Figure 1-14 shows a straight DS-1 cable.

Note To install the right-angle DS-1 cable, you must have the screw-lock power connector installed.

Figure 1-14 Straight DS-1 Cable

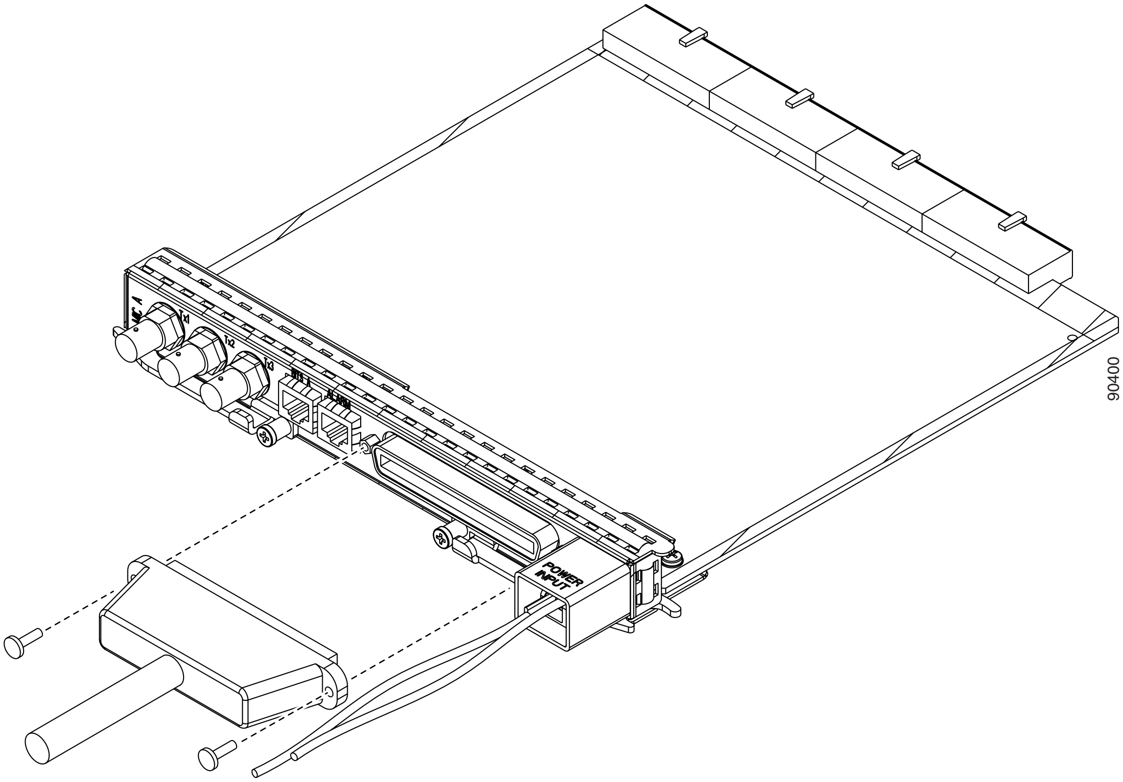
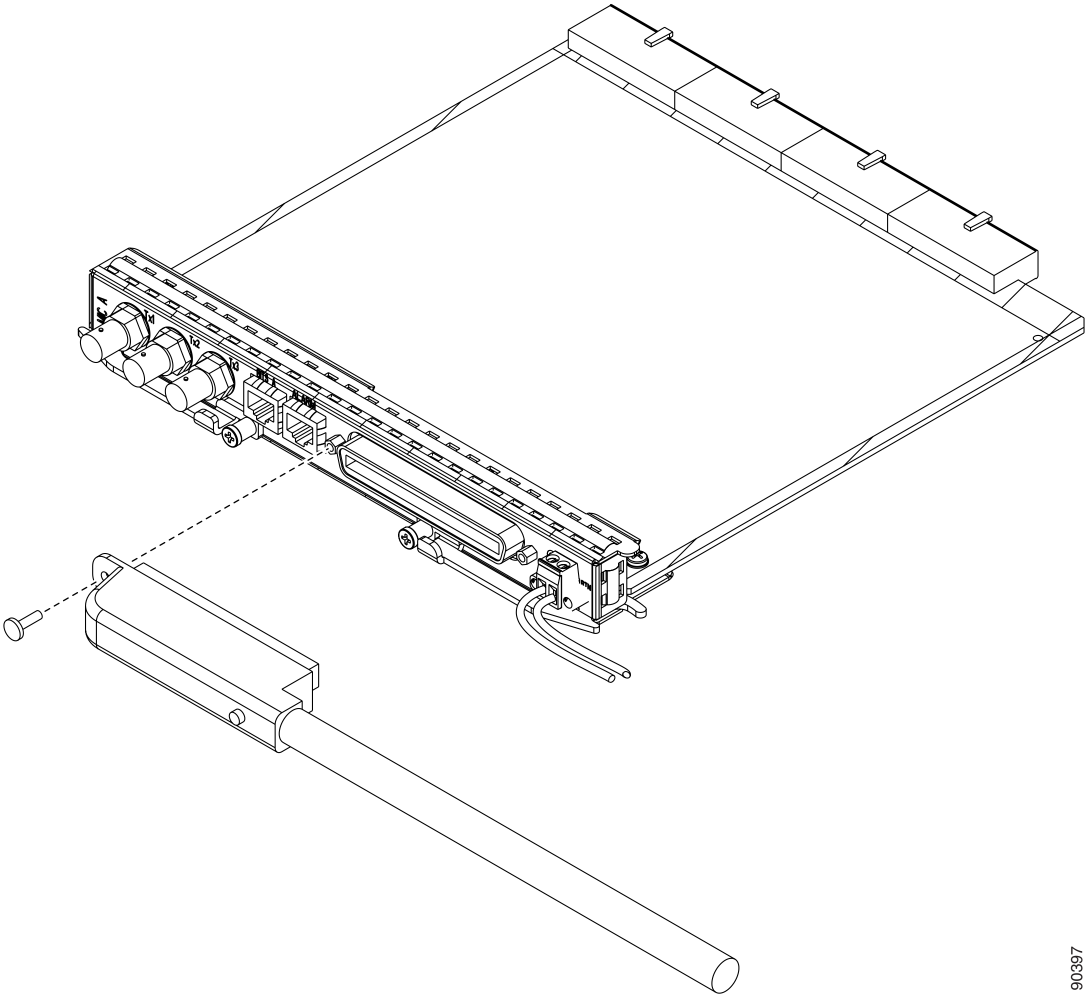


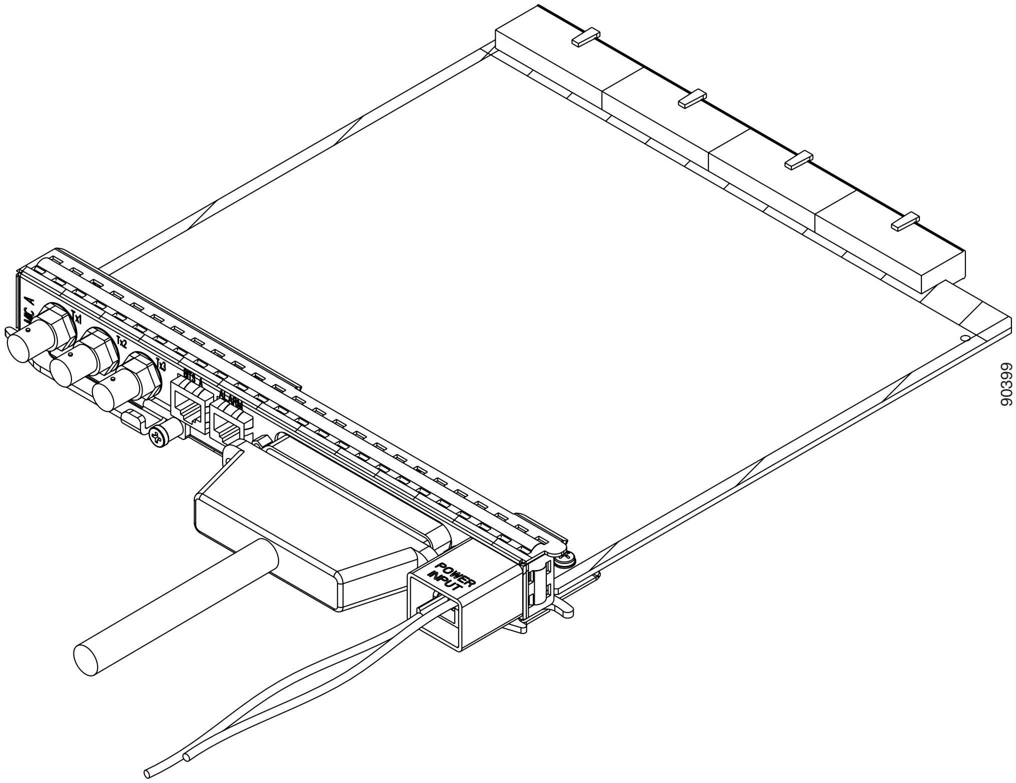
Figure 1-15 shows a right-angle DS-1 cable.

Figure 1-15 Right-Angle DS-1 Cable



Step 3 Use the screws on the male connector to secure the connection. Figure 1-16 shows a straight DS-1 cable installation.

Figure 1-16 Installing a Straight DS-1 Cable



Step 4 Return to your originating procedure (NTP).

DLP-B325 Install Coaxial Cable With BNC Connectors

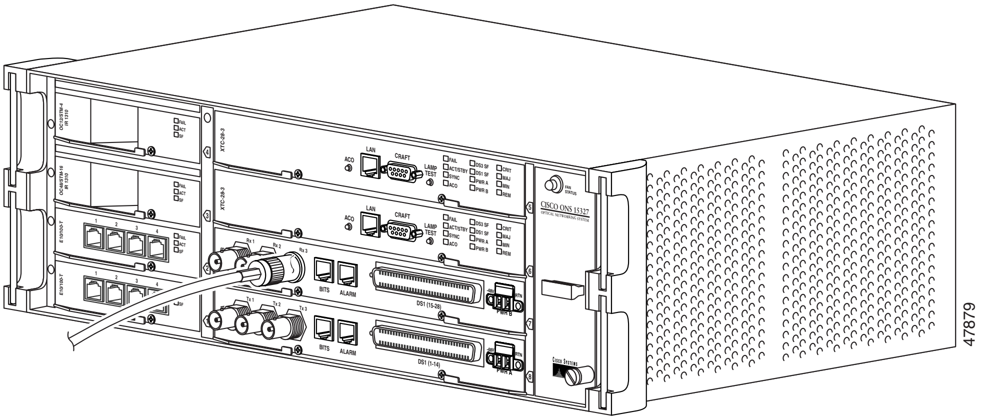
Purpose	This task installs the coaxial cable with BNC connectors to connect DS-3 signals to the ONS 15327.
Tools/Equipment	Shielded coaxial cable terminated with BNC connectors for DS-3 ports
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

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

Step 1 Place a BNC cable connector over the connector on the MIC.

Figure 1-17 shows how to connect a coaxial cable to an ONS 15327 MIC.

Figure 1-17 Installing a Coaxial Cable with BNC Connectors



Step 2 Position the cable connector so that the slot in the connector is above the corresponding notch on the MIC connection point.

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

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

Step 5 Return to your originating procedure (NTP).

DLP-B326 Route Electrical Cables

Purpose	Use this task to route and manage electrical cables.
Tools/Equipment	None
Prerequisite Procedures	NTP-B220 Install the Electrical Cables, page 1-33
Required/As Needed	Required if using electrical cards
Onsite/Remote	Onsite
Security Level	None

Caution Because cables can be damaged or cut, Cisco recommends that you diversely route redundant cables along different paths. If you installed the tie-down bar, you can run one cable across the tie-down bar and secure it using tie-wraps or other site-specific methods. You should route the other cable in the opposite direction. You can also route the cable through the cable storage drawer. See the "NTP-B223 Install the Fiber-Optic Cable Storage Drawer" procedure on page D-2 and the "NTP-B224 Route Cables Through the Fiber-Optic Cable Storage Drawer" procedure on page D-2.

Step 1 Route the cables to the nearest side of the shelf assembly through the side cutouts according to local site practice.

Step 2 Label all cables at each end of the connection to avoid confusion with cables that are similar in appearance.

Step 3 Return to your originating procedure (NTP).

NTP-B221 Install Optical Cables

Purpose	This procedure describes how to install fiber-optic cables on optical cards and small form-factor pluggable (SFP) interfaces.
Tools/Equipment	Single-mode SC fiber jumpers with UPC polish (55 dB or better) for OC12 and OC-48 cards and fiber jumpers with LC connectors for the OC-3 card Fiber boot
Prerequisite Procedures	NTP-B218 Install the Optical and Ethernet Cards, page 1-23
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

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

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

Note You can install the fiber immediately after installing the cards, or wait until you are ready to turn up the network. See Chapter 4, "Turn Up Network."

Note Inspect and clean all fiber connectors thoroughly. See the "NTP-B112 Clean Fiber Connectors" procedure on page 14-20 for instructions. Dust particles can degrade performance. Put caps on any fiber connectors that are not used.

Note To install fiber-optic cables in the ONS 15327, a fiber cable with the corresponding connector type must be connected to the transmit and receive ports on the ONS 15327 cards.

Step 1 Test the optical receive levels for the installed cards and attenuate them accordingly. See Table 1-6 for the minimum and maximum levels.

Table 1-6 Optical Transmit and Receive Levels

	Transmit		Receive	
Card	Minimum	Maximum	Minimum	Maximum
OC3 IR 4 1310	–15 dBm	–8 dBm	–28 dBm	–8 dBm
OC12 IR 1310	–15 dBm	–8 dBm	–29 dBm	–7 dBm
OC12 LR 1550	–3 dBm	+2 dBm	–29 dBm	–7 dBm
OC48 IR 1310	–5 dBm	0 dBm	–18 dBm	–0 dBm
OC48 LR 1310	–2 dBm	+3 dBm	–28 dBm	–8 dBm

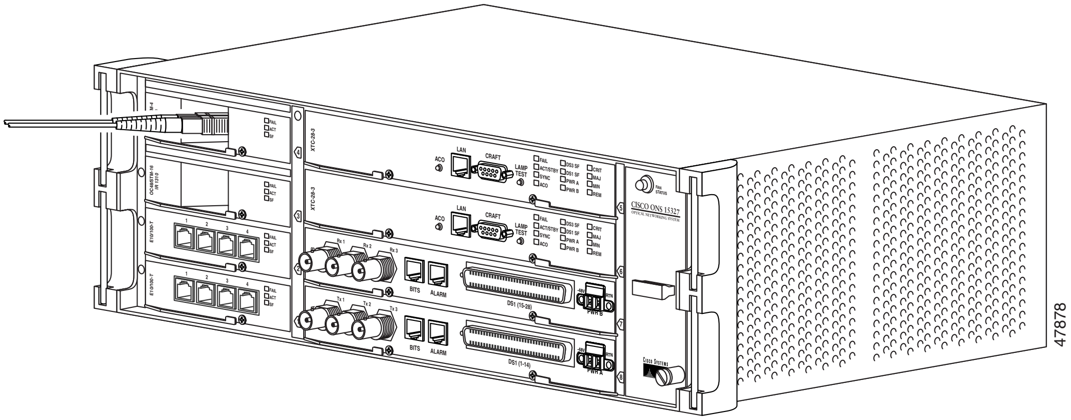
Step 2 As needed, complete the "DLP-B327 Install Fiber-Optic Cables on the LGX Interface" task on page 1-42. Figure 1-18 shows the cable location.

Step 3 As needed, complete the "DLP-B42 Install Fiber-Optic Cables on OC-N Cards" task on page 1-42.

Step 4 As needed, complete the "DLP-B43 Install Fiber-Optic Cables for UPSR Configurations" task on page 1-43.

Step 5 As needed, complete the "DLP-B44 Install Fiber-Optic Cables for BLSR Configurations" task on page 1-46.

Figure 1-18 Installing a Fiber-Optic Cable



Step 6 As needed, complete the "DLP-B46 Route Fiber-Optic Cables" task on page 1-47.

Step 7 Continue with the "NTP-B13 Perform the Shelf Installation Acceptance Test" task on page 1-48.

Stop. You have completed this procedure.

DLP-B327 Install Fiber-Optic Cables on the LGX Interface

Purpose	This task installs fiber-optic cables on the Lightguide Cross Connect (LGX) interface in the Central Office.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-B218 Install the Optical and Ethernet Cards, page 1-23 NTP-B112 Clean Fiber Connectors, page 14-20
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note Inspect and clean all fiber connectors thoroughly. See the "NTP-B112 Clean Fiber Connectors" procedure on page 14-20 for instructions. Dust particles can degrade performance. Put caps on any fiber connectors that are not used.

Step 1 Align the keyed ridge of the cable connector with the receiving SC connector on the LGX faceplate connection point. Each module supports at least one transmit and one receive connector to create an optical carrier port.

Step 2 Gently insert the cable connector into the faceplate connection point until the connector snaps into place.

Step 3 Connect the fiber optic cable to the OC-N card. See the "DLP-B42 Install Fiber-Optic Cables on OC-N Cards" task on page 1-42.

Step 4 Return to your originating procedure (NTP).

DLP-B42 Install Fiber-Optic Cables on OC-N Cards

Purpose	This task installs fiber-optic cables on optical (OC-N) cards.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-B218 Install the Optical and Ethernet Cards, page 1-23 NTP-B112 Clean Fiber Connectors, page 14-20 DLP-B327 Install Fiber-Optic Cables on the LGX Interface, page 1-42 (as applicable)
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note Inspect and clean all fiber connectors thoroughly. See the "NTP-B112 Clean Fiber Connectors" procedure on page 14-20 for instructions. Dust particles can degrade performance. Put caps on any fiber connectors that are not used.

Note ONS 15327 OC-12 and OC-48 cards have SC connectors and the OC-3 and G1000-2 cards have LC connectors. On ONS 15327 OC-12 and OC-48 card ports, the left connector is the transmit port and the right connector is the receive port.

Step 1 Align the keyed ridge of the cable connector with the receiving connector on the faceplate connection point. Each card supports at least one transmit and one receive connector to create an optical carrier port.

Step 2 Gently insert the cable connector into the faceplate connection point until the connector snaps into place.

Step 3 Return to your originating procedure (NTP).

DLP-B43 Install Fiber-Optic Cables for UPSR Configurations

Purpose	This task installs the fiber-optic cables to the east and west UPSR ports at each node. See Chapter 4, "Turn Up Network" to provision and test UPSR configurations.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-B218 Install the Optical and Ethernet Cards, page 1-23 NTP-B112 Clean Fiber Connectors, page 14-20
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note To avoid error, connect fiber-optic cable so that the highest slot in the shelf represents the east port, and the lowest slot represents the west port. Fiber connected to an east port at one node must plug into the west port on an adjacent node.

Note Inspect and clean all fiber connectors thoroughly. See the "NTP-B112 Clean Fiber Connectors" procedure on page 14-20 for instructions. Dust particles can degrade performance. Put caps on any fiber connectors that are not used.

Note You can install the fiber immediately after installing the cards, or wait until you are ready to turn up the network. See Chapter 4, "Turn Up Network."

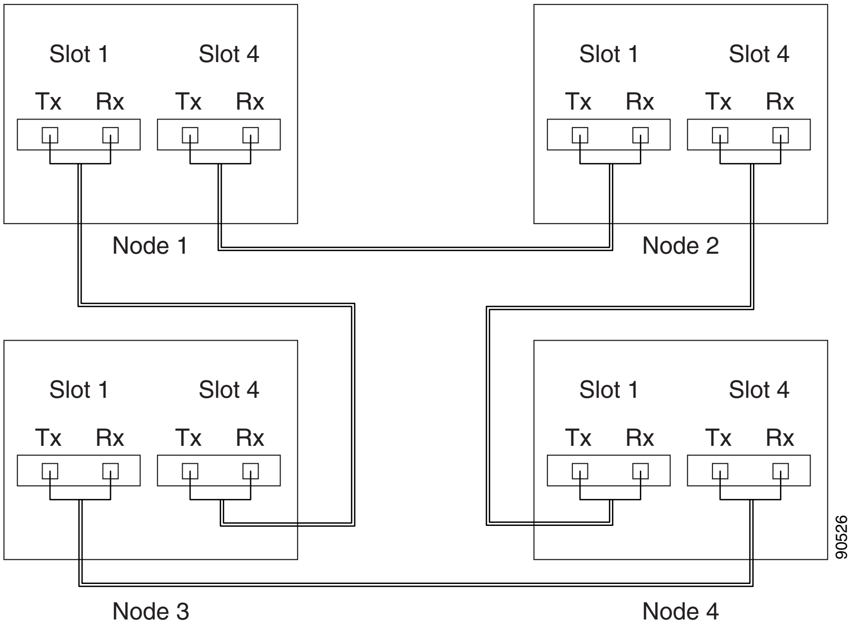
Step 1 Plan your fiber connections. Use the same plan for all UPSR nodes.

Step 2 Plug the fiber into the transmit (Tx) connector of an OC-N card at one node and plug the other end of the fiber into the receive (Rx) connector of an OC-N card at the adjacent node. The card will display a signal fail (SF) LED if the transmit and receive fibers are mismatched (for example, one fiber connects a receive port on one card to a receive port on another card).

Step 3 Repeat Step 2 until you have configured the entire ring.

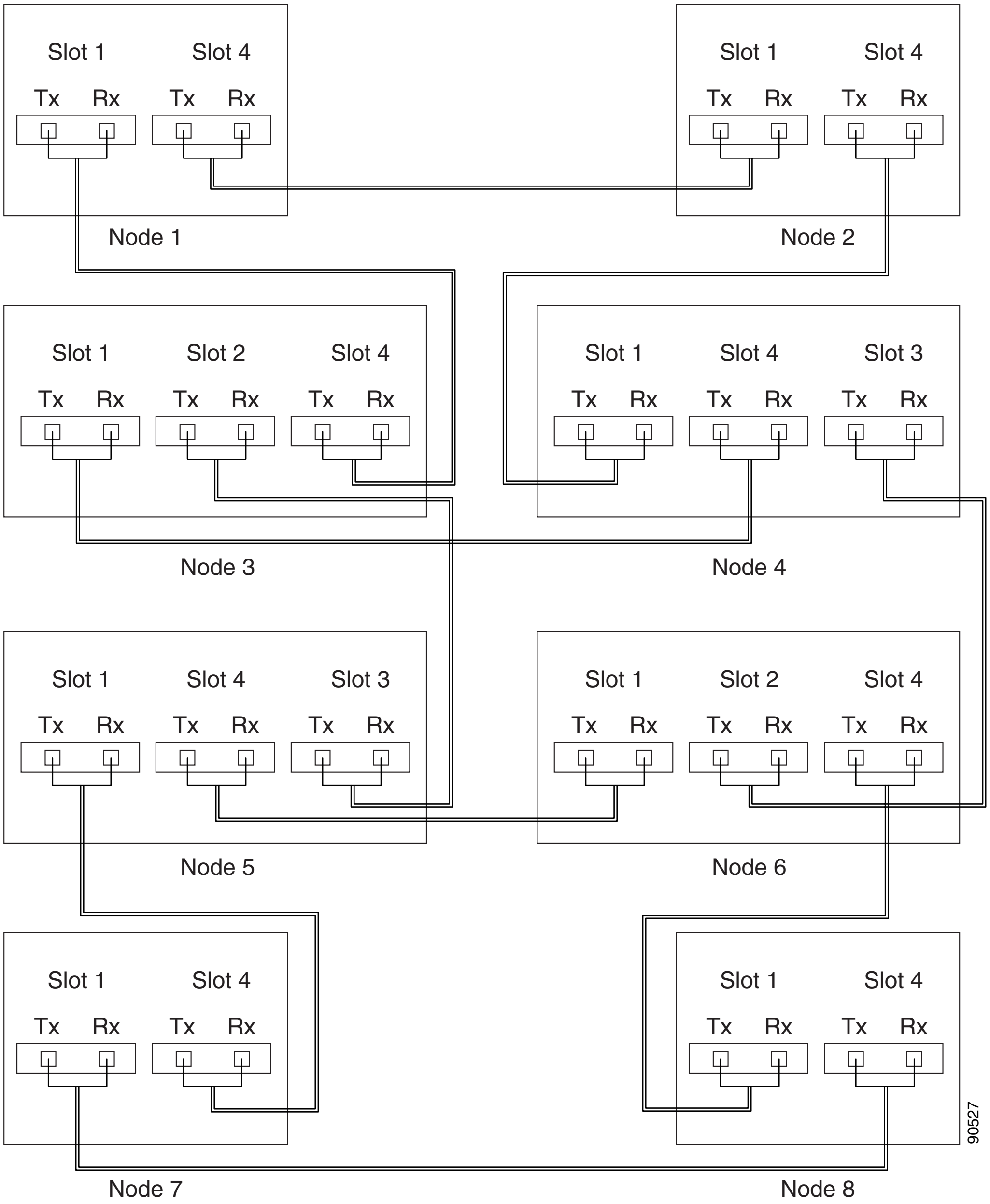
Figure 1-19 shows fiber connections for a four-node UPSR with trunk (span) cards in Slot 5 (west) and Slot 12 (east).

Figure 1-19 Connecting Fiber to a Four-Node UPSR



If you are creating a UPSR dual ring interconnect, Figure 1-20 shows a traditional dual ring interconnect example.

Figure 1-20 Connecting Fiber to an Eight-Node Traditional UPSR Dual-Ring Interconnect



Step 4 Return to your originating procedure (NTP).

DLP-B44 Install Fiber-Optic Cables for BLSR Configurations

Purpose	This task installs the fiber-optics to the east and west BLSR ports at each node. See Chapter 4, "Turn Up Network" to provision and test BLSR configurations.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-B218 Install the Optical and Ethernet Cards, page 1-23 NTP-B112 Clean Fiber Connectors, page 14-20
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note To avoid error, connect fiber-optic cable so that the highest slot on the 15327 chassis represents the east port, and the lowest slot represents the west port. Fiber connected to an east port at one node must plug into the west port on an adjacent node.

Note Inspect and clean all fiber connectors thoroughly. See the "NTP-B112 Clean Fiber Connectors" procedure on page 14-20 for instructions. Dust particles can degrade performance. Put caps on any fiber connectors that are not used.

Note You can install the fiber immediately after installing the cards, or wait until you are ready to turn up the network. See Chapter 4, "Turn Up Network."

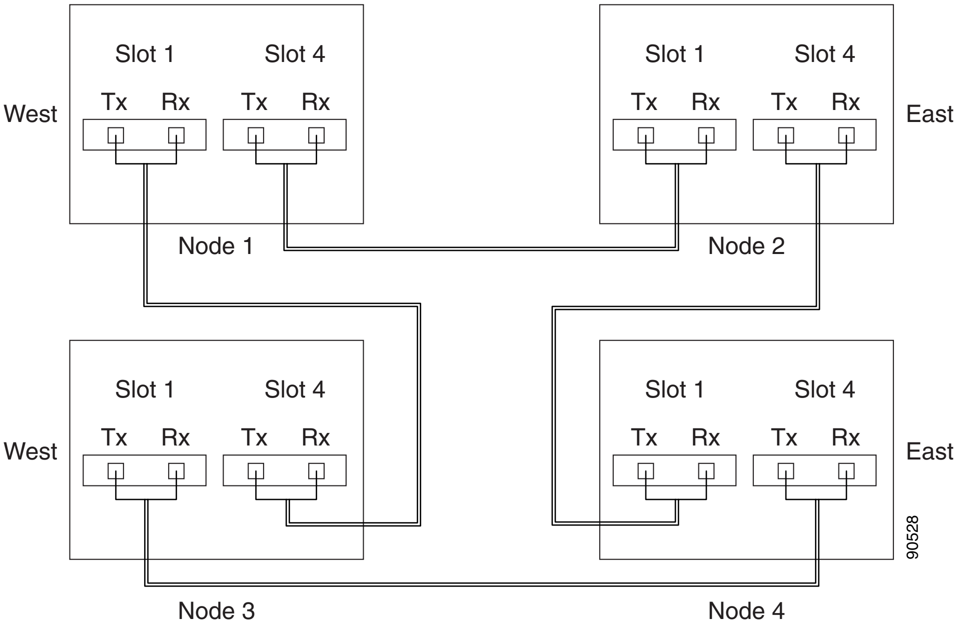
Step 1 Plan your fiber connections. Use the same plan for all BLSR nodes.

Step 2 Plug the fiber into the transmit (Tx) connector of an OC-N card at one node and plug the other end into the receive (Rx) connector of an OC-N card at the adjacent node. The card will display a signal fail (SF) LED if the transmit and receive fibers are mismatched.

Step 3 Repeat Step 2 until you have configured the entire ring.

Figure 1-21 shows fiber connections for a BLSR with trunk (span) cards in Slot 5 (west) and Slot 12 (east).

Figure 1-21 Connecting Fiber to a Four-Node, Two-Fiber BLSR



Step 4 Return to your originating procedure (NTP).

DLP-B46 Route Fiber-Optic Cables

Purpose	This task describes how to route fiber-optic cables through the cable guides on the sides of the shelf assembly.
Tools/Equipment	None
Prerequisite Procedures	NTP-B221 Install Optical Cables, page 1-40
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Caution Because an optical cable can be damaged or cut, Cisco recommends that you diversely route redundant cables along different paths. If you installed the tie-down bar, you can run one cable across the tie-down bar and secure it using tie-wraps or other site-specific methods. You should route the other cable in the opposite direction. You can also route the cable through the cable storage drawer. See the “NTP-B223 Install the Fiber-Optic Cable Storage Drawer” procedure on page D-2 and the “NTP-B224 Route Cables Through the Fiber-Optic Cable Storage Drawer” procedure on page D-2.

Step 1 Locate the cable guides on either side of the shelf assembly.

Step 2 Gently route the fiber cables through the cable guides.

Step 3 Return to your originating procedure (NTP).

NTP-B13 Perform the Shelf Installation Acceptance Test

Purpose	Use this procedure to perform a shelf installation acceptance test.
Tools/Equipment	Voltmeter
Prerequisite Procedures	Chapter 1, "Install Hardware"
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Step 1 Complete Table 1-7 on page 1-48 by verifying that each procedure was completed.

Table 1-7 ONS 15327 Shelf Installation Task Summary

Description	Completed
NTP-B1 Unpack and Inspect the ONS 15327 Shelf Assembly, page 1-4	
NTP-B2 Install the Shelf Assembly, page 1-5	
NTP-B216 Install the Mechanical Interface Cards, page 1-11	
NTP-B6 Install the Power and Ground, page 1-12	
NTP-B7 Install the Fan-Tray Assembly, page 1-20	
NTP-B217 Install the XTCs, page 1-21	
NTP-B218 Install the Optical and Ethernet Cards, page 1-23	
NTP-B8 Install Wires to Alarm, Timing, LAN, and Craft Pin Connections, page 1-28	
NTP-B220 Install the Electrical Cables, page 1-33	
NTP-B221 Install Optical Cables, page 1-40	

Step 2 Check each wire and cable connection to make sure all cables are locked securely. If a wire or cable is loose, return to the appropriate procedure in this chapter to correct it.

Step 3 Complete the "DLP-B33 Measure Voltage" task on page 1-49.

Stop. You have completed this procedure.

DLP-B33 Measure Voltage

Purpose	This task measures power so you can verify correct power and returns.
Tools/Equipment	Voltmeter
Prerequisite Procedures	NTP-B6 Install the Power and Ground, page 1-12 Table 1-7 on page 1-48.
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Using a voltmeter, verify the office ground and power shows the power terminals):

a. Place the black lead (positive) on the frame ground on the rack. Hold it there while completing Step b.

b. Place the red lead (negative) on the fuse power points and alarm panel to verify that they read between -42 VDC and -57 VDC (power) and 0 (return ground).

Step 2 Using a voltmeter, verify the shelf ground and power wiring:

a. Place the black lead (positive) on the RET1 and the red lead on the BAT1 point. Verify a reading between -42 VDC and -57 VDC. If there is no voltage, check the following:

- Battery and ground reversed to the shelf
- Battery is open or missing
- Return is open or missing

b. Repeat Step 2 for the RET2 and BAT2 if the B power feed is provided.

Step 3 Return to your originating procedure (NTP).

Connect the PC and Log into the GUI

This chapter explains how to connect PCs and workstations to the Cisco ONS 15327 and how to log into Cisco Transport Controller (CTC) software, the Cisco ONS 15327 Operation, Administration, Maintenance, and Provisioning (OAM&P) user interface.

Before You Begin

This section lists the chapter procedures (NTPs). Review the procedure for applicable tasks (DLPs).

1. NTP-B21 Set Up Computer for CTC, page 2-1—Complete this procedure if your PC or workstation has never been connected to an ONS 15327.
2. NTP-B22 Set Up CTC Computer to Connect to the ONS 15327, page 2-8—After your PC or workstation is set up for CTC, complete this procedure to set up your computer to connect to the ONS 15327.
3. NTP-B23 Log into the ONS 15327 GUI, page 2-22—Complete this procedure to log into CTC.

NTP-B21 Set Up Computer for CTC

Purpose	This procedure explains how to configure your PC or UNIX workstation to run Cisco Transport Controller (CTC).
Tools/Equipment	Cisco ONS 15327 Release 3.4 software or documentation CD
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 If your computer is a Windows PC, complete the "DLP-B47 Run the CTC Installation Wizard for Windows" task on page 2-2, then go to Step 4.

Step 2 If your computer is a UNIX workstation, complete the "DLP-B48 Run the CTC Installation Wizard for UNIX" task on page 2-5.

Step 3 If your computer is a UNIX workstation and you installed the JRE in Step 2, complete the "DLP-B49 Set Up the Java Runtime Environment for UNIX" task on page 2-7.

Step 4 When your PC or workstation is set up, complete the "NTP-B22 Set Up CTC Computer to Connect to the ONS 15327" procedure on page 2-8.

Stop. You have completed this procedure.

DLP-B47 Run the CTC Installation Wizard for Windows

Purpose	This task installs CTC online help as well as programs required to run CTC on Windows PCs: Netscape 4.73 and JRE 1.3.1_02. It also modifies the Java Runtime Environment (JRE) policy file so CTC files can be downloaded to your computer when you connect to an ONS 15327.
Tools/Equipment	Cisco ONS 15327 Release 3.4 software or documentation CD
Prerequisite Procedures	None
Required/As Needed	This task is required if any one of the following is true: • Netscape Release 4.73 or later or Internet Explorer Release 4.0 (Service Pack 2) or later is not installed. • JRE 1.3.1_02 is not installed. • CTC online help is not installed and is needed. • The JRE java.policy file has not been modified for CTC.
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Verify that your computer has the following:

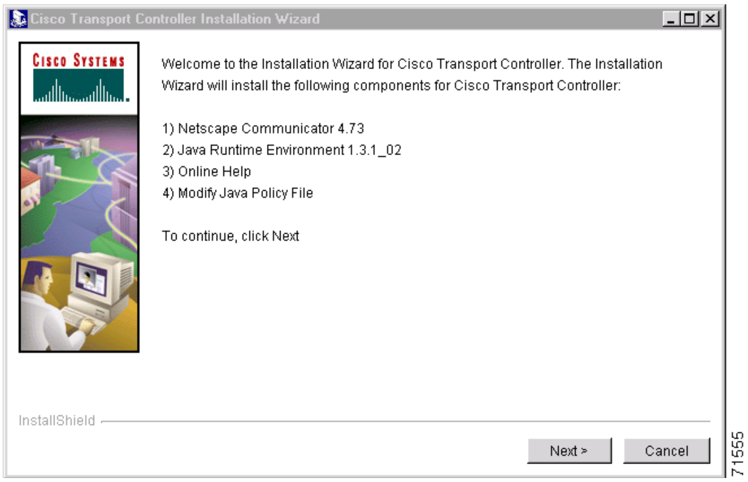
- Processor—Pentium II, 300 Mhz or faster.
- RAM—128 MB.
- Hard drive—2 GB is recommended. 50 MB of space must be available.
- Operating System—Windows 95, Windows 98, Windows NT 4.0, Windows 2000, or Windows XP. If your operating system is Windows NT, verify that Service Pack 5 or later is installed: from the Start menu, choose **Programs > Administrative Tools > Windows NT Diagnostics** and check the service pack on the Version tab of the Windows NT Diagnostics dialog box. If Service Pack 5 or later is not installed, do not continue. Install Service Pack 5 following the computer upgrade procedures for your site.

Note Processor and RAM requirements are guidelines. CTC performance will be faster if your computer has a faster processor and more RAM. Refer to the *Cisco ONS 15327 Reference Manual* for computer requirements needed for small, medium, and large ONS 15327 networks.

Step 2 Insert the Cisco ONS 15327 Release 3.4 software or documentation CD into your computer CD drive. The installation program begins running automatically. If it does not start, navigate to your computer's CD directory and double-click **setup.exe**.

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

Figure 2-1 Cisco Transport Controller Installation Wizard



Welcome to the Installation Wizard for Cisco Transport Controller. The Installation Wizard will install the following components for Cisco Transport Controller:

1) Netscape Communicator 4.73
2) Java Runtime Environment 1.3.1_02
3) Online Help
4) Modify Java Policy File

To continue, click Next

Step 3 Click **Next**.

Step 4 Choose **Typical** to install all the components shown in Figure 2-1, or choose **Custom** if you only want to install some of the components.

Step 5 Click **Next**.

Step 6 If you selected **Custom** in Step 4, select the CTC components you want to install and click **Next**. If you selected **Typical**, skip this step and proceed to Step 7.

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

a. If you do not want to change the directory, skip this step and proceed to Step 8.

b. If you want to change the CTC online help directory, type the new directory path in the Directory Name field, or click **Browse** to navigate to the directory.

Step 8 Click **Next**.

Step 9 Review the components that will be installed. If you want to change them, click **Back**. If you have an active CTC session (for example, you are monitoring alarms or conditions), close CTC before going to Step 10.

Step 10 Click **Next**.

An Installation Issues dialog box is displayed.

Step 11 Review the issues, then click **OK**. The InstallShield program begins the Netscape Communicator 4.73 Setup program.

Step 12 Complete the Netscape installation:

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

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

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

Note If the Netscape installation hangs when installing RealPlayer G2, restart the CTC installation by pressing **Ctrl-Alt-Del**. In the Windows Security dialog box, click **Task Manager.** In the Windows Task Manager dialog box, click **Cisco Transport Controller Installation Wizard**, then click the **End Task** button. Click **Yes** on the confirmation. Navigate to the drive containing the CTC CD and double-click **CTC.exe**. Repeat Steps 1 to 11. At Step 12, substep c, click **Custom**, then click **Next.** At the next panel, deselect **RealPlayer**. Continue with step d.

d. In the Netscape Desktop Preferences Options dialog box, check the boxes that apply according to your site requirements (these options will not affect CTC operation), then click **Next**.

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

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

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

h. In the Information dialog box, click **OK**.

i. In the Restarting Windows dialog box, click **No, I will restart later**, then click **OK**.

Step 13 Close the Netscape Communicator directory window to display the Cisco Transport Controller Installation Wizard dialog box.

Step 14 In the CTC Installation Wizard dialog box, click **Next**. The Java 2 runtime environment installation begins.

Step 15 Complete the JRE installation:

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

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

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

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

Step 16 Click **Next**. The CTC online help is installed. When installed, the policy file selection is displayed.

Step 17 Choose the JRE policy file to modify:

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

Step 18 Click **Next**.

Step 19 If you selected System Policy File in Step 17, complete the following steps. If you selected User Policy File, go to Step 20.

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

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

Step 20 Click **Finish**.

Step 21 Return to your originating procedure (NTP).

DLP-B48 Run the CTC Installation Wizard for UNIX

Purpose	This task installs CTC online help and programs required to run CTC on Solaris workstations: Netscape 4.76 and JRE 1.3.1_02. It also modifies the Java Runtime Environment (JRE) policy file to allow CTC files to be downloaded to your computer after you connect to an ONS 15327.
Tools/Equipment	Cisco ONS 15327 Release 3.4 software or documentation CD
Prerequisite Procedures	None
Required/As Needed	Required if any of the following are true: • Netscape Release 4.76 is not installed. • JRE 1.3.1_02 is not installed. • CTC online help is not installed and is needed. • The JRE java.policy file has not been modified for CTC.
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Verify that your computer has the following:

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

Note These requirements are guidelines. CTC performance will be faster if your computer has a faster processor and more RAM. Refer to the *Cisco ONS 15327 Reference Manual* for computer requirements needed for small, medium, and large ONS 15327 networks.

Step 2 Change the directory. Type:

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

Step 3 From the techdoc454 CD directory, type:

```
./setup.bat
```

The Cisco Transport Controller Installation Wizard displays the components that will be installed on your computer (Figure 2-1 on page 2-3):

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

Step 4 Click **Next**.

Step 5 Choose **Typical** to install all components, or choose **Custom** if you want to choose particular components to install.

Step 6 Click **Next**.

Step 7 If you selected **Custom** in Step 5, choose the CTC components you want to install and click **Next**. If you selected **Typical**, proceed to Step 8.

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

Step 9 Click **Next**.

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

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

Step 12 Complete the Netscape installation:

a. In the Netscape Communicator 4.76 Setup dialog box, click **Next**.

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

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

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

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

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

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

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

Step 14 Complete the JRE installation:

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

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

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

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

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

Step 16 Choose the JRE policy file to modify:

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

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

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

Step 18 Return to your originating procedure (NTP).

DLP-B49 Set Up the Java Runtime Environment for UNIX

Purpose	This task sets up the Java Runtime Environment (JRE) for UNIX workstations.
Tools/Equipment	None
Prerequisite Procedures	DLP-B48 Run the CTC Installation Wizard for UNIX, page 2-5
Required/As Needed	Required if you installed the JRE during the CTC installation
Onsite/Remote	Onsite or remote
Security Level	None

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

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

Step 1 Set up the environment variable:

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

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

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

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

Step 2 Set the JRE reference:

a. Run the Control Panel by typing:

```
JRE-path/j2re1_3_0_02/bin/ControlPanel
```

b. Click the **Advanced** tab.

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

```
JRE-path/j2re1_3_1_02
```

d. Click **Apply**.

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

Step 3 Return to your originating procedure (NTP).

NTP-B22 Set Up CTC Computer to Connect to the ONS 15327

Purpose	This procedure explains how to set up a PC running Windows or a Solaris workstation to connect to the ONS 15327.
Tools/Equipment	Depends on connection type
Prerequisite Procedures	NTP-B21 Set Up Computer for CTC, page 2-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 From Table 2-1, select the ONS 15327 connection type that you want to set up for your computer.

Note For initial shelf turn up, you should connect your PC directly to the LAN port on the XTC card of the ONS 15327.

Table 2-1 ONS 15327 Connection Methods

Method	Description	Requirements
Local craft	Refers to onsite network connections between the CTC computer and the ONS 15327 using: • The RJ-45 (LAN) port on the XTC, or • A hub or switch to which the ONS 15327 is connected.	If you do not use dynamic host configuration protocol (DHCP), you will need to change the computer IP address, subnet mask, and default router, or use automatic host detection.
Corporate LAN	Refers to a connection to the ONS 15327 through a corporate or network operations center (NOC) LAN.	• The ONS 15327 must be provisioned for LAN connectivity, including IP address, subnet mask, default gateway. • The ONS 15327 must be physically connected to the corporate LAN. • The CTC computer must be connected to the corporate LAN that has connectivity to the ONS 15327.
TL1	Refers to a connection to the ONS 15327 using TL1 rather than CTC. TL1 sessions can be started from CTC, or you can use a TL1 terminal. The physical connection can be a craft connection, corporate LAN, or a TL1 terminal. Refer to the *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide*.	—
Remote	Refers to a connection made to the ONS 15327 using a modem.	• A modem must be connected to the ONS 15327. • The modem must be provisioned for ONS 15327. To run CTC, the modem must be provisioned for Ethernet access.

Step 2 If you need to set up your computer for corporate LAN access, complete the "DLP-B55 Set Up a Computer for a Corporate LAN Connection" task on page 2-19. If not, proceed to the next step.

Step 3 If you need to set up the computer for remote access, complete the "DLP-B58 Provision Remote Access to the ONS 15327" task on page 2-21. If not, proceed to the next step.

Step 4 If you need to set up your computer for TL1 access, refer to the *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide*. If not, proceed to the next step.

Step 5 If you need to set up your computer for local craft connections, choose a task from Table 2-2.

Table 2-2 ONS 15327 Craft Connection Options

Local Craft Connection Task	Description
DLP-B52 Set Up a Windows PC for Craft Connection to an ONS 15327 Using Automatic Host Detection, page 2-15	Complete this task if: • All nodes that you will access run Software Release 3.3 or later. • You will connect to ONS 15327s at different locations and times and do not wish to reconfigure your PC's IP settings each time. • You do not need to access or use non-ONS 15327 applications such as ping and trace route. • You will connect to the ONS 15327's XTC Ethernet port either directly or through a hub.
DLP-B50 Set Up a Windows PC for Craft Connection to an ONS 15327 on the Same Subnet Using Static IP Addresses, page 2-11	Complete this task if: • You are connecting from a Windows PC. • You will connect to one ONS 15327; if you will connect to multiple ONS 15327s, you might need to configure your computer's IP settings each time you connect to an ONS 15327. • You need to access non-ONS 15327 applications such as ping and trace route.
DLP-B53 Set Up a Solaris Workstation for a Craft Connection to an ONS 15327, page 2-17	Complete this task if: • You are connecting from a Solaris workstation. • You will connect to one ONS 15327; if you will connect to multiple ONS 15327s, you might need to configure your computer's IP settings each time you connect to an ONS 15327. • You need to access non-ONS 15327 applications such as ping and trace route.
DLP-B51 Set Up a Windows PC for Craft Connection to an ONS 15327 Using DHCP, page 2-13	Complete this task if: • The CTC computer is provisioned for DHCP. • The ONS 15327 has DHCP forwarding enabled and is connected to a DHCP server.

Stop. You have completed this procedure.

DLP-B50 Set Up a Windows PC for Craft Connection to an ONS 15327 on the Same Subnet Using Static IP Addresses

Purpose	This task sets up your computer for a local craft connection to the ONS 15327 when: • You will access nodes running software releases before Release 3.3. • You will connect to one ONS 15327; if you will connect to multiple ONS 15327s, you might need to reconfigure your computer's IP settings each time you connect to an ONS 15327. • You need to use non-ONS 15327 applications such as ping and trace route.
Tools/Equipment	None
Prerequisite Procedures	NTP-B21 Set Up Computer for CTC, page 2-1
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

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

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

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

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

Step 2 If you have Windows 95 or 98 installed on your PC, complete the following steps:

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

b. In the Control Panel dialog box, click the **Network** icon.

c. In the Network dialog box, select **TCP/IP** for your PC Ethernet card, then click **Properties**.

d. In the TCP/IP Properties dialog box, click the **DNS Configuration** tab and choose **Disable DNS**.

e. Click the **WINS Configuration** tab and choose **Disable WINS Resolution**.

f. Click the **IP Address** tab.

g. In the IP Address window, click **Specify an IP address**.

h. In the IP Address field, enter an IP address.

i. In the Subnet Mask field, type the same subnet mask as the ONS 15327. The default is **255.255.255.0** (24 bit).

j. Click **OK**.

k. In the TCP/IP dialog box, click the **Gateway** tab.

l. In the New Gateway field, type the ONS 15327 IP address. Click **Add**.

m. Verify that the IP address appears in the Installed Gateways field, then click **OK**.

n. When the prompt to restart your PC appears, click **Yes**.

Step 3 If you have Windows NT 4.0 installed on your PC, complete the following steps:

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

b. In the Control Panel dialog box, click the **Network** icon.

c. In the Network dialog box, click the **Protocols** tab, choose **TCP/IP Protocol**, then click **Properties**.

d. Click the **IP Address** tab.

e. In the IP Address window, click **Specify an IP address**.

f. In the IP Address field, enter an IP address.

g. In the Subnet Mask field, type **255.255.255.0**.

h. Click the **Advanced** button.

i. Under the Gateways List, click **Add**. The TCP/IP Gateway Address dialog box is displayed.

j. Type the ONS 15327 IP address in the Gateway Address field.

k. Click **Add**.

l. Click **OK**.

m. Click **Apply**.

n. In some cases, Windows NT will prompt you to reboot your PC. If you receive this prompt, click **Yes**.

Step 4 If you have Windows 2000 installed on your PC, complete the following steps:

a. From the Windows Start menu, choose **Settings** > **Network and Dial-up Connections > Local Area Connection**.

b. In the Local Area Connection Status dialog box, click **Properties**.

c. In the General tab, choose **Internet Protocol (TCP/IP)**, then click **Properties**.

d. Click **Use the following IP address**.

e. In the IP Address field, enter an IP address.

f. In the Subnet Mask field, type **255.255.255.0**.

g. In the Default Gateway field, type the ONS 15327 IP address.

h. Click **OK**.

i. In the Local Area Connection Properties dialog box, click **OK**.

j. In the Local Area Connection Status dialog box, click **Close**.

Step 5 If you have Windows XP installed on your PC, complete the following steps:

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

Note If the Network Connections menu is not available, click **Switch to Classic View**.

b. In the Network Connections dialog box, click the **Local Area Connection** icon.

c. In the Local Area Connection Properties dialog box, choose **Internet Protocol (TCP/IP)**, then click **Properties**.

d. In the IP Address field, enter an IP address.

e. In the Subnet Mask field, type **255.255.255.0**.

f. In the Default Gateway field, type the ONS 15327 IP address.

g. Click **OK**.

h. In the Local Area Connection Properties dialog box, click **OK**.

i. In the Local Area Connection Status dialog box, click **Close**.

Step 6 Return to your originating procedure (NTP).

DLP-B51 Set Up a Windows PC for Craft Connection to an ONS 15327 Using DHCP

Purpose	This task sets up your computer for craft connection to the ONS 15327 using DHCP (dynamic host configuration protocol).
Tools/Equipment	Straight-through (Category 5) LAN cable
Prerequisite Procedures	NTP-B21 Set Up Computer for CTC, page 2-1 NTP-B169 Set Up CTC Network Access, page 3-7
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Caution You will not be able to connect to the ONS 15327 if DHCP forwarding is not enabled on the ONS 15327 or the ONS 15327 is not connected to a DHCP server. By default, DHCP forwarding is not enabled. If you are connecting to an ONS 15327 to perform initial shelf turn up, complete the "DLP-B50 Set Up a Windows PC for Craft Connection to an ONS 15327 on the Same Subnet Using Static IP Addresses" task on page 2-11 or the "DLP-B52 Set Up a Windows PC for Craft Connection to an ONS 15327 Using Automatic Host Detection" task on page 2-15.

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

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

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

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

Step 2 If you have Windows 95 or 98 installed on your PC, complete the following steps:

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

b. In the Control Panel dialog box, click the **Network** icon.

c. In the Network dialog box, select **TCP/IP** for your PC Ethernet card, then click **Properties**.

d. In the TCP/IP Properties dialog box, click the **DNS Configuration** tab and choose **Disable DNS**.

e. Click the **WINS Configuration** tab and choose **Disable WINS Resolution**.

f. Click the **IP Address** tab.

g. In the IP Address window, click **Obtain an IP address from a DHCP Server**.

h. Click **OK**.

i. When the prompt to restart your PC appears, click **Yes**.

Step 3 If you have Windows NT 4.0 installed on your PC, complete the following steps:

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

b. In the Control Panel dialog box, click the **Network** icon.

c. In the Network dialog box, click the **Protocols** tab, choose **TCP/IP Protocol**, then click **Properties**.

d. Click the **IP Address** tab.

e. In the IP Address window, click **Obtain an IP address from a DHCP Server**.

f. Click **OK**.

g. Click **Apply**.

h. If Windows prompts you to restart your PC, click **Yes**.

Step 4 If you have Windows 2000 installed on your PC, complete the following steps:

a. From the Windows Start menu, choose **Settings** > **Network and Dial-up Connections > Local Area Connection**.

b. In the Local Area Connection Status dialog box, click **Properties**.

c. In the General tab, choose **Internet Protocol (TCP/IP)**, then click **Properties**.

d. Click **Obtain an IP address from a DHCP Server**.

e. Click **OK**.

f. In the Local Area Connection Properties dialog box, click **OK**.

g. In the Local Area Connection Status dialog box, click **Close**.

Step 5 If you have Windows XP installed on your PC, complete the following steps:

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

Note If the Network Connections menu is not available, click **Switch to Classic View**.

b. In the Network Connections dialog box, click **Local Area Connection**.

c. In the Local Area Connection Status dialog box, click **Properties**.

d. In the General tab, choose **Internet Protocol (TCP/IP)**, then click **Properties**.

e. Click **Obtain an IP address automatically**.

f. Click **OK**.

g. In the Local Area Connection Properties dialog box, click **OK**.

h. In the Local Area Connection Status dialog box, click **Close**.

Step 6 Return to your originating procedure (NTP).

DLP-B52 Set Up a Windows PC for Craft Connection to an ONS 15327 Using Automatic Host Detection

Purpose	This task sets up your computer for local craft connection to the ONS 15327 when: • You will connect to the ONS 15327's Ethernet port or through a hub. • All nodes that you will access are running Software Release 3.3 or higher. • You will connect to multiple ONS 15327s and do not want to reconfigure your IP address each time. • You do not need to access non-ONS 15327 applications such as ping and trace route.
Tools/Equipment	None
Prerequisite Procedures	NTP-B21 Set Up Computer for CTC, page 2-1
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note If you are using automatic host detection and you disconnect a straight-through (Category 5) LAN cable from one node and connect it to another node, you must close CTC and relaunch it to reconnect to the proxy server and communicate with the new node.

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

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

Note In Windows XP, you can select Control Panel directly from the Start menu. Make sure you are in Classic View before continuing with this procedure.

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

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

Step 2 If you have Windows 95 or 98 installed on your PC, complete the following steps:

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

b. In the Control Panel dialog box, click the **Network** icon.

c. In the Network dialog box, select **TCP/IP** for your PC Ethernet card, then click **Properties**.

d. In the TCP/IP Properties dialog box, click the **DNS Configuration** tab and choose **Disable DNS**.

e. Click the **WINS Configuration** tab and choose **Disable WINS Resolution**.

f. Click the **IP Address** tab.

g. In the IP Address window, click **Specify an IP address**.

h. In the IP Address field, enter any legitimate IP address other than the node IP address of the ONS 15327.

i. In the Subnet Mask field, type the same subnet mask as the ONS 15327. The default is **255.255.255.0** (24 bit).

j. Click **OK**.

k. In the TCP/IP dialog box, click the **Gateway** tab.

l. In the New Gateway field, type the address entered in Step f. Click **Add**.

m. Verify that the IP address appears in the Installed Gateways field, then click **OK**.

n. When the prompt to restart your PC appears, click **Yes**.

Step 3 If you have Windows NT 4.0 installed on your PC, complete the following steps:

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

b. In the Control Panel dialog box, click the **Network** icon.

c. In the Network dialog box, click the **Protocols** tab, choose **TCP/IP Protocol**, then click **Properties**.

d. Click the **IP Address** tab.

e. In the IP Address window, click **Specify an IP address**.

f. In the IP Address field, enter any legitimate IP address other than the node IP address of the ONS 15327.

g. In the Subnet Mask field, type the same subnet mask as the ONS 15327. The default is **255.255.255.0** (24 bit).

h. Click the **Advanced** button.

i. Under the Gateways List, click **Add**. The TCP/IP Gateway Address dialog box is displayed.

j. Type the IP address entered in Step f in the Gateway Address field.

k. Click **Add**.

l. Click **OK**.

m. Click **Apply**.

n. Reboot your PC.

Step 4 If you have Windows 2000 installed on your PC, complete the following steps:

a. From the Windows Start menu, choose **Settings** > **Network and Dial-up Connections > Local Area Connection**.

b. In the Local Area Connection Status dialog box, click **Properties**.

c. In the General tab, choose **Internet Protocol (TCP/IP)**, then click **Properties**.

d. Click **Use the following IP address**.

e. In the IP Address field, enter any legitimate IP address other than the node IP address of the ONS 15327.

f. In the Subnet Mask field, type the same subnet mask as the ONS 15327. The default is **255.255.255.0** (24 bit).

g. Type the IP address entered in Step e in the Gateway Address field.

h. Click **OK**.

i. In the Local Area Connection Properties dialog box, click **OK**.

j. In the Local Area Connection Status dialog box, click **Close**.

Step 5 If you have Windows XP installed on your PC, complete the following steps:

a. From the Windows Start Menu, choose **Control Panel > Network Connections**.

> **Note** If the Network Connections menu is not available, click **Switch to Classic View**.

b. In the Network Connections dialog box, click the **Local Area Connection** icon.

c. In the Local Area Connection Properties dialog box, choose **Internet Protocol (TCP/IP)**, then click **Properties**.

d. In the IP Address field, enter any legitimate IP address other than the node IP address of the ONS 15327.

e. In the Subnet Mask field, type the same subnet mask as the ONS 15327. The default is **255.255.255.0** (24 bit).

f. Type the IP address entered in Step d in the Gateway Address field.

g. Click **OK**.

h. In the Local Area Connection Properties dialog box, click **OK**.

i. In the Local Area Connection Status dialog box, click **Close**.

Step 6 Return to your originating procedure (NTP).

DLP-B53 Set Up a Solaris Workstation for a Craft Connection to an ONS 15327

Purpose	This task sets up a Solaris workstation for a craft connection to the ONS 15327.
Tools/Equipment	None
Prerequisite Procedures	NTP-B21 Set Up Computer for CTC, page 2-1
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Log into the workstation as the root user.

Step 2 Check to see if the interface is plumbed by typing:

```
# ifconfig device
```

For example:

```
# ifconfig hme1
```

Step 3 If the interface is plumbed, a message similar to the following appears:

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

Go to Step 6.

Step 4 If the interface is not plumbed, a message similar to the following appears:

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

Plumb the interface by typing:

```
# if config device plumb
```

For example:

```
# ifconfig hme1 plumb
```

Step 5 Configure the IP address on the interface by typing:

```
# ifconfig interface ip-address netmask netmask up
```

For example:

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

Note Enter an IP address that is identical to the ONS 15327 IP address except for the last three digits. The last three digits must be between 1 and 254. In the Subnet Mask field, type 255.255.255.0. Skip this step if Craft Access Only is checked at **Provisioning** > **Network** > **General** > **Gateway Settings**.

Step 6 Test the connection:

a. Start Netscape Navigator.

b. Enter the Cisco ONS 15327 IP address in the web address (URL) field. If the connection is established, a Java Console window, CTC caching messages, and the Cisco Transport Controller Login dialog box display. If this occurs, go to Step 2 of the "DLP-B60 Log into CTC" task on page 2-23 to complete the login. If the Login dialog box does not appear, complete Steps c to d.

c. At the prompt, type:

```
ping ONS 15327 IP address
```

For example, you would type **ping 192.168.1.1** to connect to an ONS 15327 with default IP address 192.168.1.1. If your workstation is connected to the ONS 15327, an "*IP-address* is alive" message appears.

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

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

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

For example:

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

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

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

Step 7 Return to your originating procedure (NTP).

DLP-B55 Set Up a Computer for a Corporate LAN Connection

Purpose	This task sets up your computer to access the ONS 15327 through a corporate LAN.
Tools/Equipment	None
Prerequisite Procedures	NTP-B21 Set Up Computer for CTC, page 2-1
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 If your computer is connected to the corporate LAN, go to Step 2. If you changed your computer's network settings for craft access to the ONS 15327, change the settings back to the corporate LAN access settings. This generally means:

- Set the IP Address in the TCP/IP dialog box back to "Obtain an IP address automatically" (Windows 95 or 98) or "Obtain an IP address from a DHCP server" (Windows NT, 2000, or XP).
- If your LAN requires that domain name system (DNS) or workplace information system (WINS) be enabled, change the setting on the DNS Configuration or WINS Configuration tab of the TCP/IP dialog box.

Step 2 If your computer is connected to a proxy server, disable proxy service or add the ONS 15327 nodes as exceptions. To disable proxy service, complete the task for the web browser you use:

- DLP-B56 Disable Proxy Service Using Internet Explorer (Windows), page 2-20, or
- DLP-B57 Disable Proxy Service Using Netscape (Windows and UNIX), page 2-20

Step 3 Return to your originating procedure (NTP).

DLP-B56 Disable Proxy Service Using Internet Explorer (Windows)

Purpose	This task disables proxy service for PCs running Internet Explorer.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	Required if your computer is connected to a network computer proxy server and your browser is Internet Explorer.
Onsite/Remote	Onsite or remote
Security Level	None

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

Note If you computer is running Windows XP, you can select Control Panel directly from the Start menu. Make sure you are in Classic View before continuing with this procedure.

Step 2 In the Control Panel window, choose **Internet Options**.

Step 3 From the Internet Properties dialog box, click **Connections** > **LAN Settings**.

Step 4 In the LAN Settings dialog box, complete one of the following:

- Deselect **Use a proxy server** to disable the service.
- Leave **Use a proxy server** selected and click **Advanced**. In the Proxy Setting dialog box under Exceptions, enter the IP addresses of ONS 15327 nodes that you will access. Separate each address with a semicolon. You can insert an asterisk for the host number to include all the ONS 15327s on your network. Click **OK** to close each open dialog box.

Step 5 Return to your originating procedure (NTP).

DLP-B57 Disable Proxy Service Using Netscape (Windows and UNIX)

Purpose	This task disables proxy service for PCs and UNIX workstations running Netscape.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	Required if your computer is connected to a network computer proxy server and your browser is Netscape.
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Open Netscape.

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

Step 3 In the Preferences dialog box under Category, choose **Advanced > Proxies**.

Step 4 On the right side of the Preferences dialog box under Proxies, complete one of the following:

- Choose **Direct connection to the Internet** to bypass the proxy server.
- Choose **Manual proxy configuration** to add exceptions to the proxy server, then click **View**. In the Manual Proxy Configuration dialog box under Exceptions, enter the IP addresses of the ONS 15327 nodes that you will access. Separate each address with a comma. Click **OK** to close each open dialog box.

Step 5 Return to your originating procedure (NTP).

DLP-B58 Provision Remote Access to the ONS 15327

Purpose	This task connects an ONS 15327 using a LAN modem.
Tools/Equipment	Modem and modem documentation
Prerequisite Procedures	NTP-B21 Set Up Computer for CTC, page 2-1
Required/As Needed	Required to access the Cisco Transport Controller
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 Connect the modem to the RJ-45 (LAN) port on the XTC.

Step 2 While referring to the modem documentation, complete the following tasks to provision the modem for the ONS 15327:

- For CTC access, set the modem for Ethernet access.
- Assign an IP address to the modem that is on the same subnet as the ONS 15327.
- The IP address the modem assigns to the CTC computer must be on the same subnet as the modem and the ONS 15327.

Note For assistance on provisioning specific modems, contact the Cisco Technical Assistance Center.

Step 3 Return to your originating procedure (NTP).

NTP-B23 Log into the ONS 15327 GUI

Purpose	Use this procedure to log into the Cisco Transport Controller, the graphical user interface software used to manage the ONS 15327. This procedure includes optional node login tasks.
Tools/Equipment	None
Prerequisite Procedures	NTP-B21 Set Up Computer for CTC, page 2-1 NTP-B22 Set Up CTC Computer to Connect to the ONS 15327, page 2-8
Required/As Needed	Required to access the Cisco Transport Controller
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 If the computer is not connected to the ONS 15327, complete the "DLP-B59 Connect Computer to the ONS 15327" task on page 2-22.

Step 2 Complete the "DLP-B60 Log into CTC" task on page 2-23.

Note For information about navigating in CTC, see Appendix A, "CTC Information and Shortcuts."

Step 3 As needed, complete the "DLP-B61 Create Login Node Groups" task on page 2-25. Login node groups display nodes that are not connected to the login node via data communications channel (DCC).

Step 4 As needed, complete the "DLP-B62 Add a Node to the Current Session or Login Group" task on page 2-26.

Stop. You have completed this procedure.

DLP-B59 Connect Computer to the ONS 15327

Purpose	This task connects a CTC computer to the ONS 15327.
Tools/Equipment	Straight-through (Category 5) LAN cable
Prerequisite Procedures	NTP-B21 Set Up Computer for CTC, page 2-1 NTP-B22 Set Up CTC Computer to Connect to the ONS 15327, page 2-8
Required/As Needed	Required to access the Cisco Transport Controller
Onsite/Remote	Onsite or remote
Security Level	None

Step 1 If your computer is set up for a local craft connection, connect a straight-through (Category 5) LAN cable from the PC or Solaris workstation network interface card (NIC) card to one of the following:

- The RJ-45 (LAN) port on the XTC
- The RJ-45 (LAN) port on a hub or switch to which the ONS 15327 is physically connected

Note For instructions on crimping your own straight-through (Category 5) LAN cables, refer to the *Cisco ONS 15327 Troubleshooting Guide*.

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

Step 3 Return to your originating procedure (NTP).

DLP-B60 Log into CTC

Purpose	This task logs into the Cisco Transport Controller, the graphical user interface software used to manage the ONS 15327.
Tools/Equipment	None
Prerequisite Procedures	NTP-B21 Set Up Computer for CTC, page 2-1 NTP-B22 Set Up CTC Computer to Connect to the ONS 15327, page 2-8
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note For information about CTC views and navigation, see Appendix A, “CTC Information and Shortcuts.”

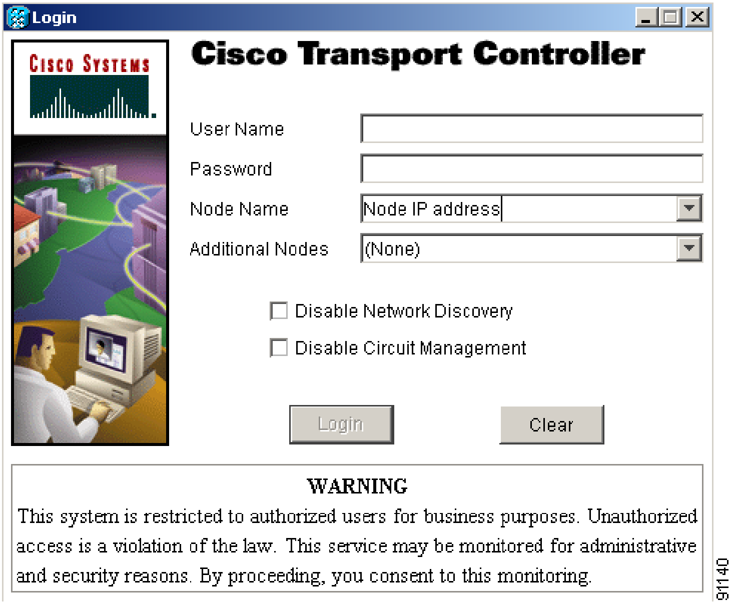
Step 1 From the PC connected to the ONS 15327, start Netscape or Internet Explorer.

Step 2 In the Netscape or Internet Explorer web address (URL) field, enter the ONS 15327 IP address. For initial setup, the default address is 192.1.0.2. Press **Enter**.

Note If you are logging into ONS 15327 nodes running different releases of CTC software, log into the node running the most recent release. If you log into a node with an older release, you receive an INCOMPATIBLE-SW alarm and the IP address of the login node appears instead of the node name. To check the software version of a node, select **About CTC** from the CTC Help menu. To resolve an alarm, refer to the *Cisco ONS 15327 Troubleshooting Guide*.

A Java Console window displays the CTC file download status. The web browser displays information about your Java and system environments. If this is the first login, CTC caching messages display while CTC files are downloaded to your computer. The first time you connect to an ONS 15327, this process can take several minutes. After the download, the CTC Login dialog box appears (Figure 2-2).

Figure 2-2 Logging into CTC



Login

Cisco Transport Controller

User Name

Password

Node Name: Node IP address

Additional Nodes: (None)

□ Disable Network Discovery

□ Disable Circuit Management

WARNING

This system is restricted to authorized users for business purposes. Unauthorized access is a violation of the law. This service may be monitored for administrative and security reasons. By proceeding, you consent to this monitoring.

Step 3 In the Login dialog box, type a user name and password (both are case sensitive). For initial setup, type the user name CISCO15.

Note The CISCO15 user is provided with every ONS 15327. CISCO15 has superuser privileges, so you can create other users. You must create another superuser before you can delete the CISCO15 user. CISCO15 is delivered without a password. To create a password for CISCO15, click the **Provisioning** > **Security** tabs after you log in and change the password. To set up ONS 15327 users and assign security, go to the "NTP-B30 Create Users and Assign Security" procedure on page 3-3. Additional information is provided in the *Cisco ONS 15327 Reference Manual*.

Step 4 Each time you log into an ONS 15327, you can make selections for the following login options:

- Node Name—Displays the IP address entered in the web browser and a drop-down menu of previously entered ONS 15327 IP addresses. You can select any ONS 15327 on the list for the login, or you can enter the IP address (or node name) of any new node where you want to log in.
- Additional Nodes—Displays a list of login node groups that are created. To create a login node group or add additional groups, see the "DLP-B61 Create Login Node Groups" task on page 2-25.

  Note Topology hosts that were created in previous ONS 15327 releases by modifying the ctc.ini (Windows) or .ctcrc (UNIX) files are displayed as a Topology Host group under Additional Nodes.

- Disable Network Discovery—Check this box to view only the ONS 15327 (and login node group members, if any) entered in the Node Name field. Nodes linked to the Node Name ONS 15327 through the DCC are not displayed. Using this option can decrease the CTC startup time in networks with many DCC-connected nodes.

- Disable Circuit Management—Check this box to disable discovery of existing circuits. Using this option can decrease the CTC initialization time in networks with many existing circuits. This option does not prevent the creation and management of new circuits.

Step 5 Click **Login**.

If login is successful, the CTC window appears. From here, you can navigate to other CTC views to provision and manage the ONS 15327. If you need to perform the initial shelf turn-up, see Chapter 3, "Turn Up Node." If login problems occur, refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 6 Return to your originating procedure (NTP).

DLP-B61 Create Login Node Groups

Purpose	This task creates a login node group to display ONS 15327s that have an IP connection but not a DCC connection to the login node.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23 NTP-B21 Set Up Computer for CTC, page 2-1 NTP-B22 Set Up CTC Computer to Connect to the ONS 15327, page 2-8
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Edit menu, choose **Preferences**.

Step 2 Click **Login Node Group** and **Create Group**.

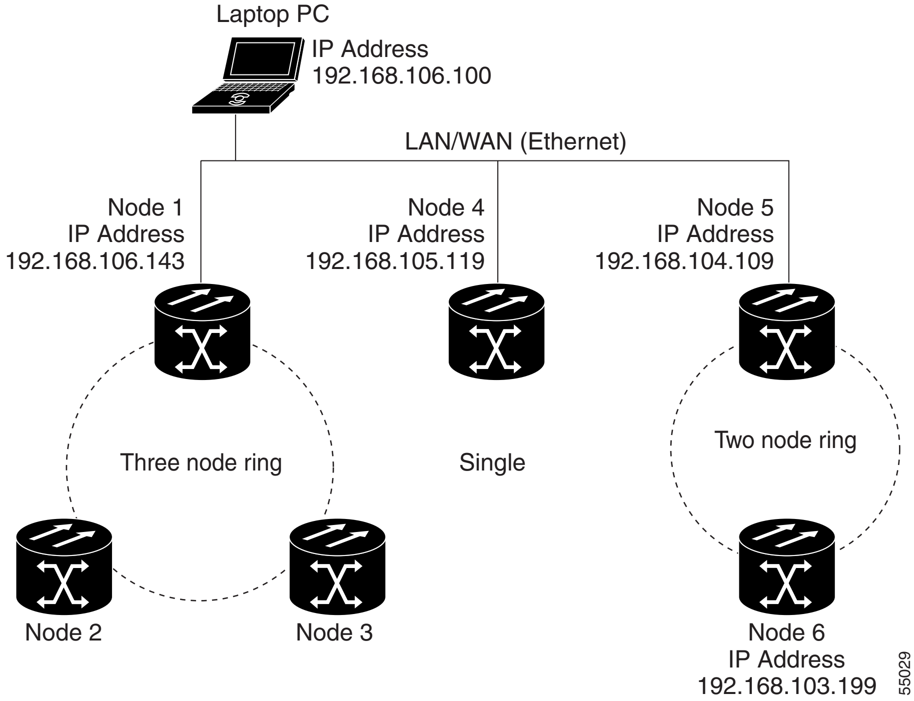
Step 3 Enter a name for the group in the Create Login Group Name dialog box. Click **OK**.

Step 4 Under Members, type the IP address (or node name) of a node you want to add to the group. Click **Add**. Repeat this step for each node you want to add to the group.

Step 5 Click **OK**.

The next time you log into an ONS 15327, the login node group will be available in the Additional Nodes list of the Login dialog box. For example, in Figure 2-3, a login node group, Test Group, is created and the IP addresses for Nodes 1, 4, and 5. During login, if you select Test Group under Additional Nodes and Disable Network Discovery is not selected, all nodes in the figure are displayed. If Test Group and Disable Network Discovery are both selected, Nodes 1, 4, and 5 are displayed. You can create as many login groups as you need. The groups are stored in the CTC preferences file on your local drive and are not visible to other users on a different CTC PC or workstation.

Figure 2-3 Login Node Group



Step 6 Return to your originating procedure (NTP).

DLP-B62 Add a Node to the Current Session or Login Group

Purpose	This task adds a node to the current CTC session or login node group.
Tools	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into an ONS 15327 on the network. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. If you are already logged in, go to Step 2.

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

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

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

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

Step 5 Click **OK**.

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

Step 6 Return to your originating procedure (NTP).

Turn Up Node

This chapter explains how to provision a single Cisco ONS 15327 node and turn it up for service, including assigning a node name, date and time, SONET timing references, network attributes such as IP address and default router, users and user security, and card protection groups.

Before You Begin

Complete the procedures applicable to your site plan from the following chapters:

- Chapter 1, “Install Hardware”
- Chapter 2, “Connect the PC and Log into the GUI”

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-B24 Verify Card Installation, page 3-2—Complete this procedure first.
2. NTP-B30 Create Users and Assign Security, page 3-3—Complete this procedure to create CTC users and assign their security levels.
3. NTP-B25 Set Up Name, Date, Time, and Contact Information, page 3-5—Continue with this procedure to set the node name, date, time, location, and contact information.
4. NTP-B169 Set Up CTC Network Access, page 3-7—Continue with this procedure to provision the IP address, default router, subnet mask, and network configuration settings.
5. NTP-B27 Set Up the ONS 15327 for Firewall Access, page 3-13—Continue with this procedure if the ONS 15327 will be accessed behind firewalls.
6. NTP-B28 Set Up Timing, page 3-16—Continue with this procedure to set up the node’s SONET timing references.
7. NTP-B170 Create Optical Protection Groups, page 3-20—Complete this procedure, as needed, to set up optical protection groups for ONS 15327 cards.
8. NTP-B171 Set Up SNMP, page 3-21—Complete this procedure if SNMP will be used for network monitoring.

NTP-B24 Verify Card Installation

Purpose	This procedure verifies that the ONS 15327 node is ready for turn up.
Tools/Equipment	An engineering work order, site plan, or other document specifying the ONS 15327 card installation
Prerequisite Procedures	Chapter 1, "Install Hardware"
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Step 1 Verify that two XTC are installed.

Step 2 Verify that the green ACT (active) LED is illuminated on one XTC and the amber STBY (standby) LED is illuminated on the second XTC.

Note If the XTCs are not installed, or their LEDs are not illuminated as described, do not proceed. Repeat the "NTP-B217 Install the XTCs" procedure on page 1-21, or refer to the *Cisco ONS 15327 Troubleshooting Guide* to resolve installation problems before proceeding to Step 3.

Step 3 Verify that OC-N cards (OC-3, OC-12, and OC-48) and Ethernet cards (E10/100 and G1000-2), if required, are installed in the slots designated by your site plan.

Step 4 Verify that all installed OC-N and Ethernet cards display a solid green ACT LED.

Step 5 Verify that fiber-optic cables are installed and connected to the locations indicated in the site plan. If the fiber-optic cables are not installed, complete the "NTP-B221 Install Optical Cables" procedure on page 1-40.

Step 6 Verify that fiber is routed correctly in the shelf assembly. If the fiber is not routed on the shelf assembly, complete the "DLP-B46 Route Fiber-Optic Cables" task on page 1-47.

Step 7 Continue with the "NTP-B25 Set Up Name, Date, Time, and Contact Information" procedure on page 3-5.

Stop. You have completed this procedure.

NTP-B30 Create Users and Assign Security

Purpose	This procedure creates ONS 15327 users and assigns their security levels.
Tools/Equipment	None
Prerequisite Procedures	NTP-B24 Verify Card Installation, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at the node where you need to create users. If you are already logged in, continue with Step 2.

Note You must log in as a Superuser to create additional users. The CISCO15 user provided with each ONS 15327 can be used to set up other ONS 15327 users. You can add up to 500 users to one ONS 15327.

Step 2 Complete the "DLP-B74 Create a New User - Single Node" task on page 3-3 or the "DLP-B75 Create a New User - Multiple Nodes" task on page 3-4 as needed.

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

Step 3 If you want to modify the security policy settings, complete the "NTP-B205 Modify Users and Change Security" procedure on page 10-17.

Stop. **You have completed this procedure**.

DLP-B74 Create a New User - Single Node

Purpose	This task creates a new user for one ONS 15327.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view, click the **Provisioning** > **Security** > **Users** tabs.

Step 2 In the Security window, click **Create**.

Step 3 In the Create User dialog box, enter the following:

- Name—Type the user name. The name must have a minimum of six and a maximum of 20 alphanumeric characters (a-z, A-Z, 0-9). For TL1 compatibility, the user name must have 6 to 10 characters, and the first character must be an alpha character.

- Password—Type the user password. The password must be a minimum of six and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) and special characters (+, #,%), where at least two characters are non-alphabetic and at least one character is a special character. For TL1 compatibility, the password must have 6 to 10 characters, and the first character must be an alpha character. The password cannot contain the user name.
- Confirm Password—Type the password again to confirm it.
- Security Level—Choose a security level for the user: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. Refer to the *Cisco ONS 15327 Reference Manual* for information about the capabilities provided with each level.

Note The idle time is the length of time that CTC can remain idle before it locks up and the password must be reentered. Each security level has a different idle time: Retrieve user = unlimited, Maintenance user = 60 minutes, Provisioning user = 30 minutes, and Superuser = 15 minutes.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-B75 Create a New User - Multiple Nodes

Purpose	This task adds a new user to multiple ONS 15327s.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note All nodes where you want to add users must be accessible in network view.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning** > **Security > Users** tabs.

Step 3 In the Security window, click **Create**.

Step 4 In the Create User dialog box, enter the following:

- Name—Type the user name. The name must have a minimum of six and a maximum of 20 alphanumeric characters (a-z, A-Z, 0-9). For TL1 compatibility, the user name must have no more than 10 characters, and the first character must be an alpha character.
- Password—Type the user password. The password must have a minimum of six and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) and special characters (+, #,%), where at least two characters are non-alphabetic and at least one character is a special character. For TL1 compatibility, the password must be 6 to 10 characters, and the first character must be an alpha character. The password cannot contain the user name.
- Confirm Password—Type the password again to confirm it.

- Security Level—Choose a security level for the user: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. Refer to the *Cisco ONS 15327 Reference Manual* for information about the capabilities provided with each level.

Note The idle time is the length of time that CTC can remain idle before it locks up and the password must be reentered. Each security level has a different idle time: Retrieve user = unlimited, Maintenance user = 60 minutes, Provisioning user = 30 minutes, and Superuser = 15 minutes.

Step 5 Under "Select applicable nodes," deselect any nodes where you do not want to add the user (all network nodes are selected by default).

Step 6 Click **OK**.

Step 7 On the User Creation Results dialog box, click **OK**.

Step 8 Return to your originating procedure (NTP).

NTP-B25 Set Up Name, Date, Time, and Contact Information

Purpose	This procedure provisions identification information for the node, including the node name, a contact name and phone number, the location of the node, and the date, time, and time zone.
Tools/Equipment	None
Prerequisite Procedures	NTP-B24 Verify Card Installation, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 for the node you will turn up. If you are already logged in, continue with Step 2.

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

Step 3 Enter the following information in the fields listed:

- Node Name—Type a name for the node. For TL1 compliance, names must begin with an alpha character and have no more than 20 alphanumeric characters.
- Contact—Type the name of the node contact person and the contact phone number up to 255 characters (optional).
- Latitude—Enter the node latitude: N (North) or S (South), degrees, and minutes (optional).
- Longitude—Enter the node longitude: E (East) or W (West), degrees, and minutes (optional).

Tip You can also position nodes manually on the network view map. Press **Ctrl** while you drag and drop the node icon to the desired location.

CTC uses the latitude and longitude to position ONS 15327 icons on the network view map. To convert a coordinate in degrees to degrees and minutes, multiply the number after the decimal by 60. For example, the latitude 38.250739 converts to 38 degrees, 15 minutes (.250739 x 60 = 15.0443, rounded to the nearest whole number).

- Description—Type a description of the node. The description can have a maximum of 255 characters.
- Use NTP/SNTP Server—When checked, CTC uses a Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) server to set the date and time of the node.

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

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

If you check the Use NTP/SNTP Server check box, type the IP address of either

- an NTP/SNTP server, or
- an ONS 15327 with NTP/SNTP Server enabled.

If you enable a firewall for the ONS 15327 proxy server, external ONS 15327 network elements (ENEs) must reference the gateway ONS 15327 for NTP/SNTP timing. For more information about the proxy server feature, refer to the *Cisco ONS 15327 Reference Manual*.

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

- Date—If the Use NTP/SNTP Server check box is not selected, type the current date in the format mm/dd/yyyy, for example, September 24, 2002 is 09/24/2002.
- Time—If the Use NTP/SNTP Server check box is not selected, type the current time in the format hh:mm:ss, for example, 11:24:58. The ONS 15327 uses a 24-hour clock, so 10:00 PM is entered as 22:00:00.
- Time Zone—Click the field and choose a city within your time zone from the popup menu. The menu displays the 80 World Time Zones from -11 through 0 (GMT) to +14. Continental United States time zones are GMT-05:00 (Eastern), GMT-06:00 (Central), GMT-07 (Mountain), and GMT-08 (Pacific).

Step 4 Click **Apply**.

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

Step 6 Review the node information. If you need to make corrections, repeat Steps 3 to 5 to enter the corrections. If the information is correct, continue with the "NTP-B169 Set Up CTC Network Access" procedure on page 3-7.

Stop. You have completed this procedure.

NTP-B169 Set Up CTC Network Access

Purpose	This procedure provisions network access for a node, including its subnet mask, default router, Dynamic Host Configuration Protocol (DHCP) server, IIOP listener port, proxy server settings, static routes, open shorted path first (OSPF) protocol, and routing information protocol (RIP).
Tools/Equipment	None
Prerequisite Procedures	NTP-B24 Verify Card Installation, page 3-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-B249 Provision IP Settings" task on page 3-7 to provision the ONS 15327 IP address, subnet mask, default router, DHCP server, IIOP listener port, and proxy server settings.

Step 3 If static routes are needed, complete the "DLP-B65 Create a Static Route" task on page 3-9. Refer to the *Cisco ONS 15327 Reference Manual* for further information about static routes.

Step 4 If the ONS 15327 is connected to a LAN or WAN that uses OSPF, complete the "DLP-B250 Set Up or Change Open Shortest Path First Protocol" task on page 3-10.

Step 5 If the ONS 15327 is connected to a LAN or WAN that uses RIP, complete the "DLP-B251 Set Up or Change Routing Information Protocol" task on page 3-12.

Stop. You have completed this procedure.

DLP-B249 Provision IP Settings

Purpose	This task provisions IP settings, which includes the IP address, default router, DHCP access, firewall access, and proxy server settings for an ONS 15327 node.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

⚠ **Caution** All network changes should be approved by your network (or LAN) administrator.

Step 1 If you are in network view, switch to node view by double-clicking the node you want to turn up on the network map.

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

Step 3 Complete the following information in the fields listed:

- IP Address—Type the IP address assigned to the ONS 15327 node.
- Suppress CTC IP Display—Check this check box if you want to prevent the node IP address from being displayed in CTC to users with Provisioning, Maintenance, or Retrieve security levels. (The IP address suppression will not be applied to users with Superuser security level.)
- Default Router—If the ONS 15327 must communicate with a device on a network that the ONS 15327 is not connected to, the ONS 15327 can forward the packets to the default router. Type the IP address of the router in this field. If the ONS 15327 is not connected to a LAN, or if you will enable any of the gateway settings to implement the ONS 15327 proxy server features, leave this field blank.
- Forward DHCP Request To—Check this check box to enable Dynamic Host Configuration Protocol (DHCP). Also, enter the DHCP server IP address in the Request To field. The check box is unchecked by default. If you will enable any of the gateway settings to implement the ONS 15327 proxy server features, leave this field blank.

  Note If you enable DHCP, computers connected to an ONS 15327 node can obtain temporary IP addresses from an external DHCP server. The ONS 15327 only forwards DHCP requests; it does not act as a DHCP server.

- MAC Address—(read only) Displays the ONS 15327 IEEE 802 Media Access Control (MAC) address.
- Net/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. The subnet mask length is the same for all ONS 15327s in the same subnet.
- XTC CORBA (IIOP) Listener Port—Check this check box to enable the ONS 15327 IIOP listener port. This listener port enables communication with the ONS 15327 through firewalls. See the "NTP-B27 Set Up the ONS 15327 for Firewall Access" procedure on page 3-13 for more information.
- Gateway Settings—Provides three check boxes that enable the ONS 15327 proxy server features. Do not check any of the check boxes until you review the proxy server scenario in the *Cisco ONS 15327 Reference Manual*. In proxy server networks, the ONS 15327 will be either a gateway network element (GNE) or end network element (ENE). Provisioning must be consistent for each NE type.
  - Craft Access Only— If checked, the login ONS 15327 is only visible to the CTC workstation that it is directly connected to; other non-DCC connected nodes will not be aware of the node provisioned for craft access only. This box is normally checked for ENEs and not checked for GNEs. If Craft Access Only is checked, Enable Proxy must be selected in order for the directly connected PC to have visibility to DCC-connected nodes.
  - Enable Proxy—If checked, the ONS 15327 responds to CTC requests with a list of DCC-connected nodes for which the node serves as a proxy. GNEs and ENEs within a proxy server network should have this check box selected.
  - Enable Firewall—If checked, the node prevents IP traffic from being routed between the DCC and the LAN port. GNEs and ENEs within a proxy server network should have this box checked. If Enable Firewall is checked, Enable Proxy must be selected in order for the directly connected PC to have visibility to DCC-connected nodes.

Step 4 Click **Apply**.

Step 5 Click **Yes** on the confirmation dialog box.

Both XTC cards will reboot, one at a time, which will take 10 to 15 minutes. Eventually, a “Lost node connection, switching to network view” message is displayed.

Step 6 Click **OK**. CTC displays the network view. The node icon is displayed in grey, during which time you cannot access the node.

Step 7 Double-click the node icon when it becomes green.

Step 8 Return to your originating procedure (NTP).

DLP-B65 Create a Static Route

Purpose	This task creates a static route to establish CTC connectivity to a computer on another network.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	Required if either of the following is true: • You need to connect ONS 15327s to CTC sessions on one subnet connected by a router to ONS 15327s residing on another subnet when OSPF is not enabled, and the Enable Proxy check box is not selected. • You need to enable multiple CTC sessions among ONS 15327s residing on the same subnet and when the Craft Access Only feature is not enabled.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu choose **Go to Network View**.

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

Step 3 Click the **Static Routing** tab. Click **Create**.

Step 4 In the Create Static Route dialog box enter the following:

- Destination—Enter the IP address of the computer running CTC. To limit access to one computer, enter the full IP address and a subnet mask of 255.255.255.255. To allow access to all computers on the 192.168.1.0 subnet, enter 192.168.1.0 and a subnet mask of 255.255.255.0. You can enter a destination of 0.0.0.0 to allow access to all CTC computers that connect to the router.
- Mask—Enter a subnet mask. If the destination is a host route (i.e., one CTC computer), enter a 32-bit subnet mask (255.255.255.255). If the destination is a subnet, adjust the subnet mask accordingly, for example, 255.255.255.0. If the destination is 0.0.0.0, CTC automatically enters a subnet mask of 0.0.0.0 to provide access to all CTC computers. You cannot change this value.
- Next Hop—Enter the IP address of the router port or the node IP address if the CTC computer is connected to the node directly.
- Cost—Enter the number of hops between the ONS 15327 and the computer.

Step 5 Click **OK**. Verify that the static route displays in the Static Route window.

Note Static route networking examples are provided in the IP networking section of the *Cisco ONS 15327 Reference Manual*.

Step 6 Return to your originating procedure (NTP).

DLP-B250 Set Up or Change Open Shortest Path First Protocol

Purpose	This task enables the Open Shortest Path First (OSPF) routing protocol on the ONS 15327. Perform this task if you want to include the ONS 15327 in OSPF-enabled networks.
Tools/Equipment	None
Prerequisite Procedures	NTP-B24 Verify Card Installation, page 3-2 DLP-B60 Log into CTC, page 2-23 You will need the OSPF Area ID, Hello and Dead intervals, and authentication key (if OSPF authentication is enabled) provisioned on the router that the ONS 15327 is connected to.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From node view, click the **Provisioning** > **Network** > **OSPF** tabs.

Step 2 On the top left side of the OSPF pane, complete the following:

- DCC/GCC OSPF Area ID Table—In dotted decimal format, enter the number that identifies the ONS 15327s as a unique OSPF area ID. It can be any number between 000.000.000.000 and 255.255.255.255. The number must be unique to the LAN OSPF area.
- DCC Metric—This value is normally unchanged. It sets a "cost" for sending packets across the DCC, which is used by OSPF routers to calculate the shortest path. This value should always be higher than the LAN metric. The default DCC metric is 10. The metric changes to 100 if you check the OSPF Active on LAN check box in Step 3.

Step 3 Under OSPF on LAN, complete the following:

- OSPF active on LAN—When checked, enables the ONS 15327 OSPF topology to be advertised to OSPF routers on the LAN. Enable this field on ONS 15327s that directly connect to OSPF routers.
- LAN Port Area ID—Enter the OSPF area ID (dotted decimal format) for the router port where the ONS 15327 is connected. (This number is different from the DCC OSPF Area ID.)

Step 4 By default, OSPF is set to No Authentication. If the OSPF router requires authentication, complete the following steps. If not, continue with Step 5.

a. Click the **No Authentication** button.

b. On the Edit Authentication Key dialog box, complete the following:

- Type—Choose **Simple Password**.
- Enter Authentication Key—Enter the password.

- Confirm Authentication Key—Enter the same password to confirm it.

c. Click **OK**.

The authentication button label changes to Simple Password.

Step 5 Verify that the OSPF priority and intervals settings match the priority and interval settings used by the OSPF router where the ONS 15327 is connected. If not, change the settings, as needed.

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

Step 6 Under OSPF Area Range Table, create an area range table if one is needed:

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

a. Under OSPF Area Range Table, click **Create**.

b. In the Create Area Range dialog box, enter the following:

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

c. Click **OK**.

Step 7 If the ONS 15327 OSPF area is not physically connected to Area 0, use the following steps to create a virtual link table that will provide the disconnected area with a logical path to Area 0:

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

b. In the Create Virtual Link dialog box, complete the following fields (OSPF settings must match OSPF settings for the ONS 15327 OSPF area):

- Neighbor—The router ID of the Area 0 router.
- Transit Delay (sec)—The service speed. One second is the default.
- Hello Int (sec)—The number of seconds between OSPF “hello” packet advertisements sent by OSPF routers. Ten seconds is the default.
- Auth Type—If the router where the ONS 15327 is connected uses authentication, choose **Simple Password**. Otherwise, choose **No Authentication**.

- Retransmit Int (sec)—Sets the time that will elapse before a packet is resent. Five seconds is the default.
- Dead Int (sec)—Sets the number of seconds that will pass while an OSPF router's packets are not visible before its neighbors declare the router down. Forty seconds is the default.

c. Click **OK**.

Step 8 After entering ONS 15327 OSPF area data, click **Apply**.

If you changed the Area ID, the XTC cards will reset, one at a time. The reset will take approximately 10 to 15 minutes. Table 3-1 on page 3-15 shows the LED behavior during the XTC reset.

Step 9 Return to your originating procedure (NTP).

DLP-B251 Set Up or Change Routing Information Protocol

Purpose	This task enables routing information protocol (RIP) on the ONS 15327. Perform this task if you want to include the ONS 15327 in RIP-enabled networks.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23 You need to create a static route to the router adjacent to the ONS 15327 if the ONS 15327 needs to communicate its routing information to non DCC-connected nodes.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From node view, click the **Provisioning** > **Network** > **RIP** tabs.

Step 2 Check the **RIP Active** check box if you are activating RIP.

Step 3 Choose either RIP Version 1 or RIP Version 2 from the pull-down menu, depending on which version is supported in your network.

Step 4 Set the RIP metric. The RIP metric can be set to a number between 1 and 15 and represents the number of hops.

Step 5 By default, RIP is set to No Authentication. If the router that the ONS 15327 is connected to requires authentication, complete the following steps. If not, continue with Step 6.

a. Click the **No Authentication** button.

b. On the Edit Authentication Key dialog box, complete the following:

- Type—choose **Simple Password**.
- Enter Authentication Key—Enter the password,
- Confirm Authentication Key—Enter the same password to confirm it.

c. Click **OK**.

The authentication button label changes to Simple Password.

Step 6 If you want to complete an address summary, complete the following steps. If not, the task is complete. Continue with Step 7. Complete the address summary only if the ONS 15327 is a GNE with multiple ONS 15327 ENEs attached with IP addresses in different subnets.

a. Under RIP Address Summary, click **Create**.

b. On the Create Address Summary dialog box, complete the following:

- Summary Address—Enter the summary IP address.
- Mask Length—Enter the subnet mask length using the up and down arrows.
- Hops—Enter the number of hops. The smaller the number of hops, the higher the priority.

c. Click **OK.**

Step 7 Return to your originating procedure (NTP).

NTP-B27 Set Up the ONS 15327 for Firewall Access

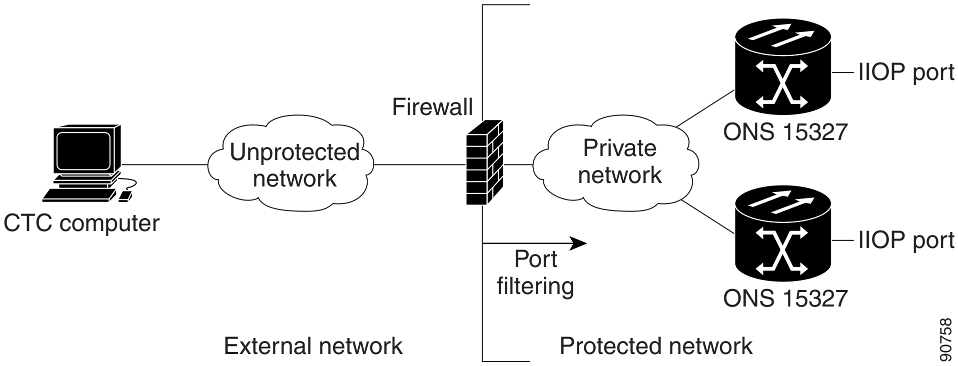
Purpose	This procedure provisions ONS 15327s and CTC computers for access through firewalls. If an ONS 15327 or CTC computer resides behind a firewall that uses port filtering, you must enable an Internet Inter-ORB Protocol (IIOP) port on the ONS 15327 and/or CTC computer, depending on whether one or both devices reside behind a firewall.
Tools/Equipment	IIOP listener port number provided by your LAN or firewall administrator
Prerequisite Procedures	NTP-B24 Verify Card Installation, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into a node that is behind the firewall. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions.

Step 2 If the ONS 15327 resides behind a firewall, complete the "DLP-B67 Provision the IIOP Listener Port on the ONS 15327" task on page 3-14.

Figure 3-1 shows an ONS 15327 in a protected network and the CTC computer in an external network. For the computer to access the ONS 15327s, you must provision the IIOP listener port specified by your firewall administrator on the ONS 15327.

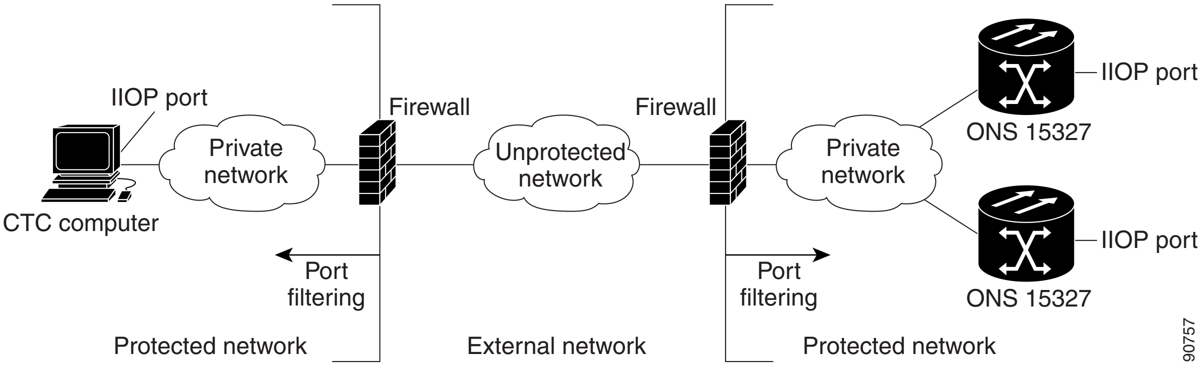
Figure 3-1 ONS 15327 Nodes Residing Behind a Firewall



Step 3 If the CTC computer resides behind a firewall, complete the "DLP-B68 Provision the IIOP Listener Port on the CTC Computer" task on page 3-16.

Figure 3-2 shows a CTC computer and ONS 15327 behind firewalls. For the computer to access the ONS 15327, you must provision the IIOP port on the CTC computer and on the ONS 15327.

Figure 3-2 A CTC Computer and ONS 15327s Residing Behind Firewalls



Stop. You have completed this procedure.

DLP-B67 Provision the IIOP Listener Port on the ONS 15327

Purpose	This task sets the IIOP listener port on the ONS 15327, which enables you to access ONS 15327s that reside behind a firewall.
Tools/Equipment	IIOP listener port number provided by your LAN or firewall administrator
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Network** tabs.

Step 2 On the **General** subtab under XTC CORBA (IIOP) Listener Port, choose a listener port option:

- Default - XTC Fixed—Select this option if the ONS 15327s are on the same side of the firewall as the CTC computer or if no firewall is used (default). This option sets the ONS 15327 listener port to Port 57790. It can be used for access through a firewall if Port 57790 is open.
- Standard Constant—Select this option to use Port 683, the CORBA default port number, as the ONS 15327 listener port.
- Other Constant—If Port 683 is not used, type the IIOP port specified by your firewall administrator. The port cannot use any of the ports shown in Table 3-1.

Table 3-1 Ports Used by the XTC Cards

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

Step 3 Click **Apply**.

Step 4 When the Change Network Configuration message appears, click **Yes**.

Both ONS 15327 XTCs will reboot, one at a time. The reboot will take approximately 10 to 15 minutes.

Step 5 Return to your originating procedure (NTP).

DLP-B68 Provision the IIOP Listener Port on the CTC Computer

Purpose	This task selects the IIOP listener port on CTC.
Tools/Equipment	IIOP listener port number provided by your LAN or firewall administrator
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, from the Edit menu choose **Preferences**.

Step 2 On the Preferences dialog box, click the **Firewall** tab.

Step 3 Under CTC CORBA (IIOP) Listener Port, choose a listener port option:

- Default - Variable—Select this option if the ONS 15327s are on the same side of the firewall as the CTC computer or if no firewall is used (default). This option sets the CTC listener port to Port 57790. It can be used for access through a firewall if Port 57790 is open.
- Standard Constant—Select this option to use Port 683, the CORBA default port number, as the CTC computer listener port.
- Other Constant—If Port 683 is not used, enter the IIOP port provided by your administrator. The port cannot be set to any port listed in Table 3-1 on page 3-15.

Step 4 Click **Apply**. A warning is displayed telling you that the port change will apply during the next CTC login.

Step 5 Click **OK**.

Step 6 On the Preferences dialog box, click **OK**. A warning appears telling you that the port change will apply during the next CTC login.

Step 7 To access the ONS 15327 using the IIOP port, log out of CTC (from the File menu, select **Exit**).

Step 8 Log into CTC. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions.

Step 9 Return to your originating procedure (NTP).

NTP-B28 Set Up Timing

Purpose	This procedure provisions the ONS 15327 timing.
Tools/Equipment	None
Prerequisite Procedures	NTP-B24 Verify Card Installation, page 3-2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into the ONS 15327 node where you want to set up timing. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. If you are already logged in, continue with Step 2.

Step 2 Complete the"DLP-B69 Set Up External or Line Timing" task on page 3-17 if an external BITS source is available. This is the most common SONET timing setup procedure.

Step 3 Complete the"DLP-B70 Set Up Internal Timing" task on page 3-19 if you cannot complete Step 2 (an external BITS source is not available). This task can only provide Stratum 3 timing.

Note For information about SONET timing, refer to the *Cisco ONS 15327 Reference Manual* or to Telcordia GR-253-CORE.

Stop. You have completed this procedure.

DLP-B69 Set Up External or Line Timing

Purpose	This task defines the external or line SONET timing source for the ONS 15327.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, click the **Provisioning > Timing** tabs.

Step 2 Under General Timing, complete the following information:

- Timing Mode—Choose **External** if the ONS 15327 derives its timing from a BITS source wired to the port on the MIC; choose **Line** if timing is derived from an OC-N card that is optically connected to the timing node. A third option, Mixed, allows you to set external and line timing references.

Note Because Mixed timing may cause timing loops, Cisco does not recommend its use. Use this mode with care.

- SSM Message Set—Choose the message set level supported by your network. If a Generation 1 node receives a Generation 2 message, the message will be mapped down to the next available Generation 1. For example, an ST3E message becomes an ST3.
- Quality of RES—If your timing source supports the reserved S1 byte, 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. Refer to the *Cisco ONS 15327 Reference Manual* for more information about SSM, including definitions of the SONET timing levels.
- Revertive—Check this check box if you want the ONS 15327 to revert to a primary reference source after the conditions that caused it to switch to a secondary timing reference are corrected.
- Reversion Time—If Revertive is checked, choose the amount of time the ONS 15327 will wait before reverting to its primary timing source. Five minutes is the default.

Step 3 Under BITS Facilities, complete the following information:

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

- State—For line-timed nodes with no equipment timed through BITS Out, set State to OOS (Out of Service). For nodes using external timing or line timing with equipment timed through BITS Out, set the state to IS (In Service).

Step 4 If the state is set to OOS, continue with Step 5. If the state is set to IS, complete the following information:

- Coding—Choose the coding used by your BITS reference, either B8ZS or AMI.
- Framing—Choose the framing used by your BITS reference, either ESF (Extended Super Frame, or SF (D4) (Super Frame).
- Sync Messaging—Check this check box to enable SSM. SSM is not available if Framing is set to Super Frame.
- AIS Threshold—If SSM is disabled or Super Frame is used, choose the quality level where a node sends an alarm indication signal (AIS) from the BITS 1 Out and BITS 2 Out backplane pins. An AIS alarm is raised when the optical source for the BITS reference falls to or below the SSM quality level defined in this field.
- LBO—If you are timing an external device connected to the BITS Out pins, choose the distance between the device and the ONS 15327. Options are: 0-133 ft. (default), 124-266 ft., 267-399 ft., 400-533 ft., and 534-655 ft.

Step 5 Under Reference Lists, complete the following information:

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

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

Step 6 Click **Apply**.

Note Refer to the *Cisco ONS 15327 Troubleshooting Guide* for timing-related alarms.

Step 7 Return to your originating procedure (NTP).

DLP-B70 Set Up Internal Timing

Purpose	This task sets up internal Stratum 3 timing for an ONS 15327.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed (use only if a BITS source is not available)
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 Under General Timing, enter the following:

- Timing Mode—Set to External
- SSM Message Set—Set to Generation 1
- Quality of RES—Not relevant to internal timing; ignore this field
- Revertive—Not relevant to internal timing; ignore this field
- Reversion Time—Not relevant to internal timing; ignore this field

Step 3 Under BITS Facilities, change State to OOS (Out of Service). Disregard the other BITS Facilities settings; they are not relevant to internal timing.

Step 4 Under Reference Lists, enter the following information:

- NE Reference
  - Ref 1—Set to Internal Clock
  - Ref 2—Set to Internal Clock
  - Ref 3—Set to Internal Clock
- BITS 1 Out/BITS 2 Out—Set to None

Step 5 Click **Apply**.

Step 6 Log into a node that will be timed from the node you set up in Steps 1 to 5.

Step 7 Click the **Provisioning > Timing** tabs.

Step 8 In the General Timing section, enter the same information as entered in Step 2 with the following exceptions:

- Timing Mode—Set to Line

Reference Lists

- NE Reference
  - Ref 1—Set to the OC-N trunk card with the closest connection to the node in Step 3
  - Ref 2—Set to the OC-N trunk card with the next closest connection to the node in Step 3
  - Ref 3—Set to Internal Clock

Step 9 Click **Apply**.

Step 10 Repeat Steps 6 through 9 at each node that will be timed by the node in Step 3.

Step 11 Return to your originating procedure (NTP).

NTP-B170 Create Optical Protection Groups

Purpose	This procedure creates ONS 15327 card protection groups.
Tools/Equipment	None
Prerequisite Procedures	NTP-B24 Verify Card Installation, page 3-2
Required/As Needed	Required; some network information is optional, depending on your site plan
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at the node where you want to create the protection group. If you are already logged in, continue with Step 2.

Step 2 From node view, click the **Provisioning** > **Protection** tabs.

Step 3 Under Protection Groups, click **Create**.

Step 4 In the Create Protection Group dialog box, enter the following:

- Name—Type a name for the protection group. The name can have up to 32 alphanumeric characters.
- Type—Choose **1+1** from the pull-down menu.
- Protect Port—Choose the protect port from the pull-down menu. The menu displays the available OC-N ports. If OC-N cards are not installed, no ports display in the pull-down menu.
- After you choose the protect port, a list of ports available for protection is displayed under Available Ports. If no cards are available, no ports are displayed. If this occurs, you will not be able to complete this task until you install the physical cards or preprovision the ONS 15327 slots.

Step 5 From the Available Ports list, choose the port that will be protected by the port you selected in Protect Ports. Click the top arrow button to move each port to the Working Ports list.

Step 6 Complete the remaining fields:

- Bidirectional switching—Check this check box if you want both Tx and Rx signals to switch to the protect port when a failure occurs to one signal. Leave it unchecked if you want only the failed signal to switch to the protect port.
- Revertive—Check this check box if you want traffic to revert to the working card after failure conditions stay corrected for the amount of time entered in the Reversion Time field.
- Reversion time—If Revertive is checked, choose the reversion time from the pull-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. Reversion time is the amount of time that will elapse before the traffic reverts to the working card. Traffic can revert when conditions causing the switch are cleared.

Step 7 Click **OK**.

Step 8 Return to your originating procedure (NTP).

NTP-B171 Set Up SNMP

Purpose	This procedure provisions the SNMP parameters so that you can use SNMP management software with the ONS 15327.
Tools/Equipment	None
Prerequisite Procedures	NTP-B24 Verify Card Installation, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at the node where you want to set up SNMP. If you are already logged in, continue with Step 2.

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

Step 3 If you want the SNMP agent to accept SNMP SET requests on certain MIBs, click the **Allow SNMP Sets** check box. If this check box is not selected, SET requests are rejected.

Step 4 Click the **Create** button.

Step 5 In the SNMP Traps Destination dialog box (Figure 3-3), complete the following:

- IP Address—Type the IP address of your network management system. If the node you are logged into is an ENE, type the IP address of the ONS 15327 GNE.
- Community Name—Type the SNMP community name. For a description of SNMP community names, refer to the SNMP information in the *Cisco ONS 15327 Reference Manual*.

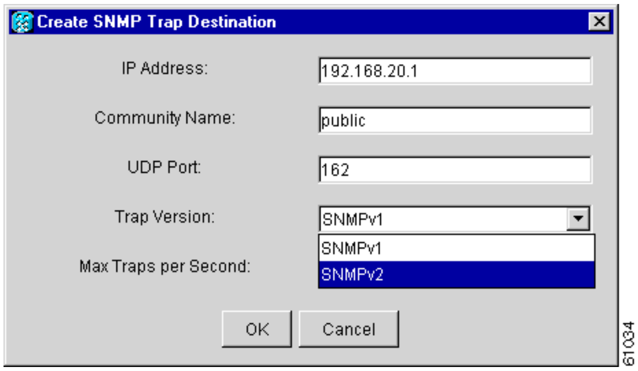
Note The community name is a form of authentication and access control. The community name assigned to the ONS 15327 is case-sensitive and must match the community name of the NMS.

- UDP Port—The default UDP port for SNMP is 162. If the node is an ENE in a proxy server network, the UDP port must be set to the GNE's SNMP relay port which is 391.

- Trap Version—Choose either SNMPv1 or SNMPv2. Refer to your NMS documentation to determine the version to use.
- Max Traps per Second—Type the maximum traps per second. The default is 0.

Note The Max Traps per Second is the maximum number of traps per second that will be sent to the SNMP manager. If the field is set to 0, there is no maximum and all traps are sent.

Figure 3-3 Setting SNMP



Create SNMP Trap Destination

IP Address: 192.168.20.1

Community Name: public

UDP Port: 162

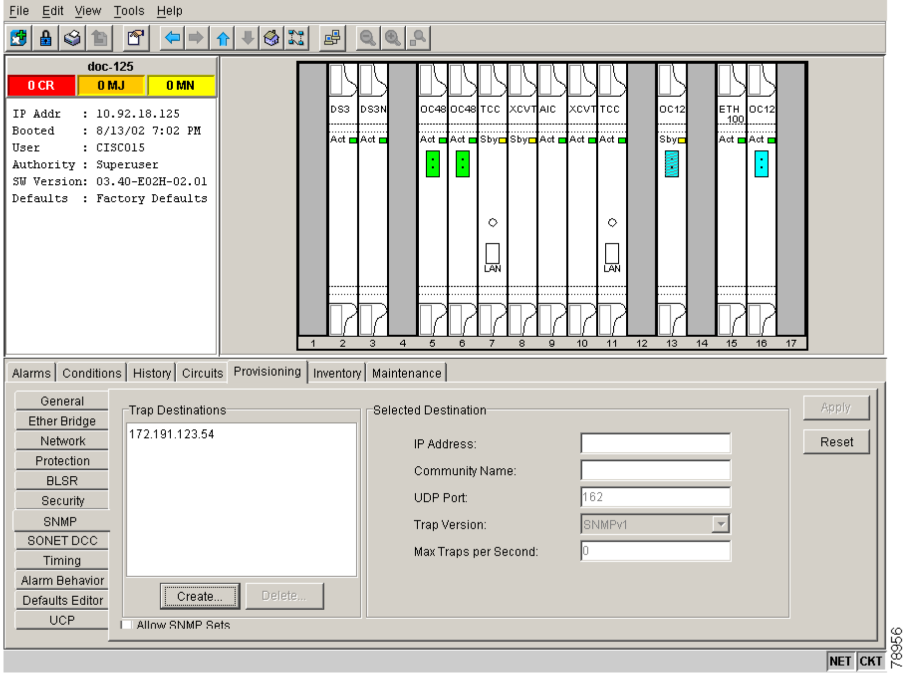
Trap Version: SNMPv1

Max Traps per Second:

Step 6 Click **OK**.

Step 7 Click the node IP address under Trap Destinations (Figure 3-4). Verify the SNMP information that appears under Selected Destination.

Figure 3-4 SNMP Trap Destinations



doc-125

0 CR 0 MJ 0 MN

```
IP Addr   : 10.92.18.125
Booted    : 8/13/02 7:02 PM
User      : CISCO15
Authority : Superuser
SW Version: 03.40-E02H-02.01
Defaults  : Factory Defaults
```

Trap Destinations

172.191.123.54

Selected Destination

IP Address:

Community Name:

UDP Port: 162

Trap Version: SNMPv1

Max Traps per Second: 0

□ Allow SNMP Sets

File Edit View Tools Help
DS3 DS3N OC48 OC48 TCC XCVT AIC XCVT TCC OC12 ETH 100 OC12
Act Act Act Act Sby Sby Act Act Act Sby Act Act
LAN
LAN
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
Alarms Conditions History Circuits Provisioning Inventory Maintenance
General
Ether Bridge
Network
Protection
BLSR
Security
SNMP
SONET DCC
Timing
Alarm Behavior
Defaults Editor
UCP
Create...
Delete...
Apply
Reset
NET CKT
78956

Stop. You have completed this procedure.

NTP-B34 Create Ethernet RMON Alarm Thresholds

Purpose	This procedure sets up remote monitoring (RMON) to allow network management systems to monitor Ethernet ports.
Tools/Equipment	None
Prerequisite Procedures	NTP-B24 Verify Card Installation, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

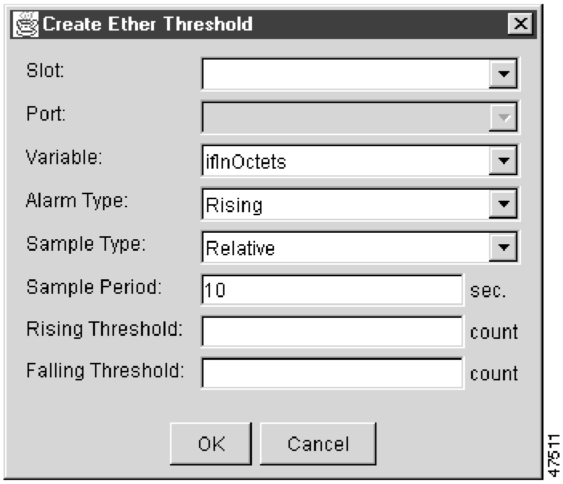
Step 1 Log into the ONS 15327 node where you want to set up SNMP. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Provisioning** > **Ether Bridge > Thresholds** tabs.

Step 3 Click **Create**.

The Create Ether Threshold dialog box opens (Figure 3-5).

Figure 3-5 Creating RMON Thresholds



Create Ether Threshold

Slot:

Port:

Variable: ifInOctets

Alarm Type: Rising

Sample Type: Relative

Sample Period: 10 sec.

Rising Threshold: count

Falling Threshold: count

Step 4 From the Slot pull-down menu, choose the appropriate Ethernet card.

Step 5 From the Port pull-down menu, choose the applicable port on the Ethernet card you selected.

Step 6 From the Variable pull-down menu, choose the variable. See Table 3-2 on page 3-24 for a list of the Ethernet threshold variables available in this field.

Step 7 From the Alarm Type pull-down menu, indicate whether the event will be triggered by the rising threshold, falling threshold, or both the rising and falling thresholds.

Step 8 From the Sample Type pull-down menu, choose either **Relative** or **Absolute**. Relative restricts the threshold to use the number of occurrences in the user-set sample period. Absolute sets the threshold to use the total number of occurrences, regardless of 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** For a rising type of alarm, the measured value must move from below the falling threshold to above the rising threshold. For example, if a network is running below a falling threshold of 400 collisions every 15 seconds and a problem causes 1001 collisions in 15 seconds, these occurrences raise an alarm.

Step 11 Enter the appropriate number of occurrences in the Falling Threshold field. In most cases a falling threshold is set lower than the rising threshold.

A falling threshold is the counterpart to a rising threshold. When the number of occurrences is above the rising threshold and then drops below a falling threshold, it resets the rising threshold. For example, when the network problem that caused 1001 collisions in 15 minutes subsides and creates only 799 collisions in 15 minutes, occurrences fall below a falling threshold of 800 collisions. This resets the rising threshold so that if network collisions again spike over a 1000 per 15 minute period, an event again triggers when the rising threshold is crossed. An event is triggered only the first time a rising threshold is exceeded (otherwise a single network problem might cause a rising threshold to be exceeded multiple times and cause a flood of events).

Step 12 Click **OK** to complete the procedure.

Table 3-2 Ethernet Threshold Variables (MIBs)

Variable	Definition
iflnOctets	Total number of octets received on the interface, including framing octets
iflnUcastPkts	Total number of unicast packets delivered to an appropriate protocol
ifInMulticastPkts	Number of multicast frames received error free
ifInBroadcastPkts	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer
ifInDiscards	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol
iflnErrors	Number of inbound packets discarded because they contain errors
ifOutOctets	Total number of transmitted octets, including framing packets
ifOutUcastPkts	Total number of unicast packets requested to transmit to a single address
ifOutMulticastPkts	Number of multicast frames transmitted error free
ifOutBroadcastPkts	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent

Table 3-2 Ethernet Threshold Variables (MIBs) (continued)

Variable	Definition
ifOutDiscards	The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted
dot3statsAlignmentErrors	Number of frames with an alignment error, i.e., the length is not an integral number of octets and the frame cannot pass the Frame Check Sequence (FCS) test
dot3StatsFCSErrors	Number of frames with framecheck errors, i.e., there is an integral number of octets, but an incorrect Frame Check Sequence (FCS)
dot3StatsSingleCollisionFrames	Number of successfully transmitted frames that had exactly one collision
dot3StatsMutlipleCollisionFrame	Number of successfully transmitted frames that had multiple collisions
dot3StatsDeferredTransmissions	Number of times the first transmission was delayed because the medium was busy
dot3StatsLateCollision	Number of times that a collision was detected later than 64 octets into the transmission (also added into collision count)
dot3StatsExcessiveCollision	Number of frames where transmissions failed because of excessive collisions
dot3StatsCarrierSenseErrors	The number of transmission errors on a particular interface that are not otherwise counted
dot3StatsSQETestErrors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface
etherStatsJabbers	Total number of Octets of data (including bad packets) received on the network
etherStatsUndersizePkts	Number of packets received with a length less than 64 octets
etherStatsFragments	Total number of packets that are not an integral number of octets or have a bad FCS, and that are less than 64 octets long
etherStatsPkts64Octets	Total number of packets received (including error packets) that were 64 octets in length
etherStatsPkts65to127Octets	Total number of packets received (including error packets) that were 65 – 172 octets in length
etherStatsPkts128to255Octets	Total number of packets received (including error packets) that were 128 – 255 octets in length
etherStatsPkts256to511Octets	Total number of packets received (including error packets) that were 256 – 511 octets in length
etherStatsPkts512to1023Octets	Total number of packets received (including error packets) that were 512 – 1023 octets in length
etherStatsPkts1024to1518Octets	Total number of packets received (including error packets) that were 1024 – 1518 octets in length
etherStatsJabbers	Total number of packets longer than 1518 octets that were not an integral number of octets or had a bad FCS

Table 3-2 Ethernet Threshold Variables (MIBs) (continued)

Variable	Definition
etherStatsCollisions	Best estimate of the total number of collisions on this segment
etherStatsCollisionFrames	Best estimate of the total number of frame collisions on this segment
etherStatsCRCAlignErrors	Total number of packets with a length between 64 and 1518 octets, inclusive, that had a bad FCS or were not an integral number of octets in length
receivePauseFrames (G series only)	The number of received 802.x pause frames
transmitPauseFrames (G series only)	The number of transmitted 802.x pause frames
receivePktsDroppedInternalCongestion (G series only)	The number of received framed dropped due to frame buffer overflow as well as other reasons
transmitPktsDroppedInternalCongestion (G series only)	The number of frames dropped in the transmit direction due to frame buffer overflow as well as other reasons
txTotalPkts	Total number of transmit packets
rxTotalPkts	Total number of receive packets

Stop. You have completed this procedure.

CHAPTER 4

Turn Up Network

This chapter explains how to turn up and test a Cisco ONS 15327 network, including terminal point-to-point networks, linear add-drop multiplexers (ADMs), unidirectional path switched rings (UPSRs), bidirectional line switched rings (BLSRs) and subtending rings.

Before You Begin

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-B35 Verify Node Turn Up, page 4-2—Complete this procedure before beginning network turn up.
2. NTP-B124 Provision a Point-to-Point Network, page 4-3—Complete as needed.
3. NTP-B173 Point-to-Point Network Acceptance Test, page 4-6—Complete this procedure after you provision a point-to-point network.
4. NTP-B38 Provision a Linear ADM Network, page 4-10—Complete as needed.
5. NTP-B174 Linear ADM Network Acceptance Test, page 4-11—Complete this procedure after you provision a linear ADM.
6. NTP-B40 Provision BLSR Nodes, page 4-13—Complete this procedure to provision ONS 15327s in a two-fiber BLSR.
7. NTP-B126 Create a BLSR, page 4-14—Complete this procedure after provisioning the BLSR nodes.
8. NTP-B175 BLSR Acceptance Test, page 4-16—Complete this procedure after you provision a two-fiber BLSR.
9. NTP-B44 Provision UPSR Nodes, page 4-22—Complete as needed.
10. NTP-B177 UPSR Acceptance Test, page 4-23—Complete this procedure after you provision a UPSR.
11. NTP-B46 Subtend a UPSR from a BLSR, page 4-25—Complete as needed.

12. NTP-B47 Subtend a BLSR from a UPSR, page 4-27—Complete as needed.
13. NTP-B48 Subtend a BLSR from a BLSR, page 4-27—Complete as needed.

NTP-B35 Verify Node Turn Up

Purpose	This procedure verifies that each ONS 15327 is ready for network turn up before adding nodes to a network.
Tools/Equipment	None
Prerequisite Procedures	Chapter 3, “Turn Up Node”
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the “DLP-B60 Log into CTC” task on page 2-23 at any node on the network you will test. If you are already logged in, proceed to Step 2.

Step 2 Click the **Alarms** tab.

a. Verify that the network does not have any unexplained alarms. If alarms are present, investigate and resolve them before continuing. Refer to the *Cisco ONS 15327 Troubleshooting Guide* for procedures.

b. Ensure that the alarm filter icon in the lower right corner is not indented. If so, click it once to turn it off. When you are done checking for alarms, click the icon again to turn alarm filtering back on. See the “DLP-B227 Disable Alarm Filtering” task on page 6-29 for instructions.

Step 3 Verify that the SW Version and Defaults displayed in the node view status area match the software version and network element (NE) defaults shown in your site plan. If any values are not correct, complete the following procedures as needed:

- If the software is not the correct version, install the correct version from the ONS 15327 software CD. Upgrade procedures are located on the CD. Follow the upgrade procedures appropriate to the software currently installed on the node.
- If the node defaults are not correct, complete the “NTP-B165 Import Network Element Defaults” procedure on page C-3.

Step 4 Click the **Provisioning > General** tabs. Verify that all general node information settings match the settings of your site plan. If not, see the “NTP-B81 Change Node Management Information” procedure on page 10-2.

Step 5 Click the **Provisioning > Timing** tabs. Verify that the timing settings match the settings on your site plan. If not, see the “NTP-B85 Change Node Timing” procedure on page 10-15.

Step 6 Click the **Provisioning > Network** tabs. Ensure that the IP settings and other CTC network access information is correct. If not, see the “NTP-B201 Change CTC Network Access” procedure on page 10-4.

Step 7 Click the **Provisioning > Protection** tabs. Verify that all protection groups have been created according to your site plan. If not, see the “NTP-B203 Modify or Delete 1+1 Card Protection Settings” procedure on page 10-12.

Step 8 Click the **Provisioning > Security** tabs. Verify that all users have been created and their security levels match the settings indicated by your site plan. If not, see the “NTP-B205 Modify Users and Change Security” procedure on page 10-17.

Step 9 If SNMP is provisioned on the node, click the **Provisioning > SNMP** tabs. Verify that all SNMP settings match the settings of your site plan. If not, see the "NTP-B87 Change SNMP Settings" procedure on page 10-23.

Stop. You have completed this procedure.

NTP-B124 Provision a Point-to-Point Network

Purpose	This procedure provisions two ONS 15327s in a point-to-point (terminal) network.
Tools/Equipment	None
Prerequisite Procedures	NTP-B35 Verify Node Turn Up, page 4-2
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Log into an ONS 15327 on the network where you want to provision a point-to-point configuration. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. If you are already logged in, continue with Step 2.

Step 2 Click the **Provisioning > Protection** tabs. Verify that 1+1 protection is created for the OC-N cards. Complete the "NTP-B170 Create Optical Protection Groups" procedure on page 3-20 if protection has not been created.

Step 3 Repeat Steps 1 and 2 for the second point-to-point node.

Step 4 Verify that the working and protect cards in the 1+1 protection groups correspond to the physical fiber connections between the nodes, that is, verify that the working card in one node connects to the working card in the other node and that the protect card in one node connects to the protect card in the other node.

Step 5 Complete the "DLP-B253 Provision SONET DCC Terminations" task on page 4-4 for the working OC-N port on both point-to-point nodes.

Note DCC terminations are not provisioned on the protect ports.

Note If the point-to-point nodes are not connected to a LAN, you will need to create the DCC terminations using a craft (direct) connection to the node. Remote provisioning is possible only after all nodes in the network have DCC terminations provisioned to in-service OC-N ports.

Step 6 Verify that timing is set up at both point-to-point nodes. If not, complete the "NTP-B28 Set Up Timing" procedure on page 3-16 for one or both of the nodes. If a node uses line timing, make its working OC-N the timing source.

Step 7 Complete the "NTP-B173 Point-to-Point Network Acceptance Test" procedure on page 4-6.

Stop. You have completed this procedure.

DLP-B253 Provision SONET DCC Terminations

Purpose	This task creates the SONET Data Communications Channel terminations required for alarms, administration, data, signal control information, and messages.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view click the **Provisioning > SONET DCC** tabs.

Step 2 Click **Create.**

Step 3 In the Create SDCC Terminations dialog box click the ports where you want to create the DCC termination. To select more than one port, press the Shift key or the Ctrl key.

Note SDCC refers to the Section DCC, which is used for ONS 15327 DCC terminations. The SONET Line DCCs and the Section DCC (when not used as a DCC termination by the ONS 15327) can be provisioned as DCC tunnels. See the "DLP-B313 Create a DCC Tunnel" task on page 5-75.

Step 4 Under Port State, click the **Set to IS** radio button.

Step 5 Verify that the Disable OSPF on DCC Link check box is unchecked.

Step 6 Click **OK**.

Note EOC (DCC Termination Failure) and LOS (Loss of Signal) alarms are present until you create all network DCC terminations and put the DCC termination OC-N ports in service.

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

Step 7 Return to your originating procedure (NTP).

DLP-B214 Change the Service State for a Port

Purpose	This task places a port in service or removes a port from service.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note To provision Ethernet ports, see the "DLP-B220 Provision E-Series Ethernet Ports" task on page 5-64 or the "DLP-B222 Provision G-Series Ethernet Ports" task on page 5-72.

Step 1 On the node view shelf graphic, double-click the card with the port(s) you want to put in or out of service. The card view appears.

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

Step 3 Under State, choose one of the following:

- IS—The port is in-service.
- OOS—The port is out-of-service. Traffic is not passed on the port until the service state is changed to IS, OOS_MT, or OOS_AINS.
- OOS_MT—The port is in a maintenance state. The maintenance state does not interrupt traffic flow, alarm reporting is suppressed, and loopbacks are allowed. Raised fault conditions, whether their alarms are reported or not, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command. Use OOS_MT for testing or to suppress alarms temporarily. Change the state to IS, OOS, or OOS_AINS when testing is complete.
- OOS_AINS—The port is in an auto-inservice state; alarm reporting is suppressed, but traffic is carried and loopbacks are allowed. Raised fault conditions, whether their alarms are reported or not, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command.

Step 4 If you change the state to OOS-AINS, set the soak period time in the AINS Soak field. This is the amount of time that the state will stay in OOS-AINS state after the signal is continuously received before changing to IS.

Note A continuously valid signal must be received for the duration of the soak period before the state makes a transition to the IS state. For example, if the soak timer is set for eight hours, and you receive an error after two hours, the timer is reset for another eight-hour period. This cycle continues until an error-free signal is received for an eight-hour period.

Step 5 Click **Apply**.

Step 6 As needed, repeat this task for each port.

Step 7 Return to your originating procedure (NTP).

NTP-B173 Point-to-Point Network Acceptance Test

Purpose	This procedure tests a point-to-point network.
Tools/Equipment	Test set/cables appropriate to the test circuit you will create
Prerequisite Procedures	NTP-B124 Provision a Point-to-Point Network, page 4-3
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Log into one of the point-to-point nodes. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. If you are already logged in, continue with Step 2.

Step 2 From the View menu choose **Go to Network View**.

Step 3 Click the **Alarms** tab.

a. Verify that the network does not have any unexplained alarms. If unexplained alarms are present, resolve them before continuing. Refer to the *Cisco ONS 15327 Troubleshooting Guide*.

b. Ensure that the alarm filter icon in the lower right corner is not indented. If so, click it once to turn it off. When you are done checking for alarms, click the icon again to turn alarm filtering back on. See the "DLP-B227 Disable Alarm Filtering" task on page 6-29 for instructions.

Step 4 Complete the "DLP-B139 Export CTC Data" task on page 6-3 to export the alarm data to a file.

Step 5 Click the **Conditions** tab. Verify that the network does not have any unexplained conditions. If unexplained conditions are present, resolve them before continuing. Refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 6 Complete the "DLP-B139 Export CTC Data" task on page 6-3 to export the condition data to a file.

Step 7 On the network map, double-click one point-to-point node to display it in node view.

Step 8 Create a test circuit from the login node to the other point-to-point node:

- For DS-1 circuits, complete the "NTP-B181 Create an Automatically Routed DS-1 Circuit" procedure on page 5-5. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For DS-3 circuits, complete the "NTP-B184 Create an Automatically Routed DS-3 Circuit" procedure on page 5-16. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.

Step 9 Configure the test set for the test circuit type you created:

- DS-1—If you are testing an unmuxed DS-1, you must have a DSX-1 panel or a direct DS-1 interface into the ONS 15327 through the AMP Champ connectors on the Mechanical Interface Card (MIC). Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- DS-3—If you are testing a clear channel DS-3, you must have a DSX-3 panel or a direct DS-3 interface into the ONS 15327 through the BNC connectors on the MIC. Set the test set for clear channel DS-3. For information about configuring your test set, consult your test set user guide.

Step 10 Verify the integrity of all patch cables that will be used in this test by connecting one end to the test set transmit (Tx) connector and the other end to the test set receive (Rx) connector. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before going to Step 11.

Step 11 Create a physical loopback at the circuit destination card. To do so, attach one end of a patch cable to the destination port transmit (Tx) connector; attach the other end to the port receive (Rx) connector.

Step 12 At the circuit source card:

a. Connect the transmit (Tx) connector of the test set to the receive (Rx) connector on the circuit source card.

b. Connect the test set receive (Rx) connector to the circuit transmit (Tx) connector on the circuit source card.

Step 13 Verify that the test set displays a clean signal. If a clean signal is not displayed, repeat Steps 8 to 12 to make sure the test set and cabling are configured correctly.

Step 14 Inject BIT errors from the test set. Verify that the errors display at the test set, indicating a complete end-to-end circuit.

Step 15 Complete the "DLP-B254 XTC Active/Standby Switch Test" task on page 4-7.

Step 16 Complete the "DLP-B88 Optical 1+1 Protection Test" task on page 4-8.

Step 17 Set up and complete a BER test. Use the existing configuration and follow your site requirements for the specified length of time. Record the test results and configuration.

Step 18 Remove any loopbacks, switches, or test sets from the nodes after all testing is complete. Refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 19 From the View menu choose **Go to Network View**.

Step 20 Click the **Alarms** tab. Verify that the network does not have any unexplained alarms. If unexplained alarms are present, resolve them before continuing. Refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 21 Repeat Steps 11 to 20 for the other point-to-point node.

Step 22 If a node fails any test, repeat the test while verifying correct setup and configuration. If the test fails again, refer to the next level of support.

Step 23 Delete the test circuit. See the "NTP-B152 Delete Circuits" procedure on page 8-13 for instructions.

After all tests are successfully completed and no alarms exist in the network, the network is ready for service application.

Stop. You have completed this procedure.

DLP-B254 XTC Active/Standby Switch Test

Purpose	This task verifies that the ONS 15327 XTC cards can effectively switch from one to another.
Tools/Equipment	The test set specified by the acceptance test procedure, connected and configured as specified in the acceptance test procedure.
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 From the View menu choose **Go to Network View**.

Step 2 Click the **Alarms** tab.

a. Verify that the network does not have any unexplained alarms. If unexplained alarms are present, resolve them before continuing. Refer to the *Cisco ONS 15327 Troubleshooting Guide*.

b. Ensure that the alarm filter icon in the lower right corner is not indented. If so, click it once to turn it off. When you are done checking for alarms, click the icon again to turn alarm filtering back on. See the "DLP-B227 Disable Alarm Filtering" task on page 6-29 for instructions.

Step 3 Click the **Conditions** tab. Verify that the network does not have any unexplained conditions. If unexplained conditions are present, resolve them before continuing. Refer to the Cisco ONS 15327 Troubleshooting Guide.

Step 4 Display the node containing the XTC cards you are testing in node view.

Step 5 Make a note of which XTC is active and which is standby by examining the LEDs on the shelf graphic. XTC cards are installed in Slot 5 and Slot 6. The active XTC has a green ACT LED, and the standby XTC has an amber SBY LED.

Step 6 On the shelf graphic, right-click the active XTC and choose **Reset** from the shortcut menu.

Step 7 On the Resetting Card dialog box, click **Yes**. After 20 to 40 seconds, a "lost node connection, changing to network view" message appears.

Step 8 Click **OK**. On the network view map, the node where you reset the XTC will be grey.

Step 9 After the node icon turns green (within 1-2 minutes), double-click it. On the shelf graphic, observe the following:

- The previous standby XTC displays a green ACT LED.
- The previous active XTC LEDs go through the following LED sequence: NP (card not present), Ldg (software is loading), amber SBY LED (XTC is in standby mode). The LEDs should complete this sequence within 5 to 10 minutes.

Step 10 Verify that traffic on the test set connected to the node is still running. If a traffic interruption occurs, do not continue, refer to your next level of support.

Step 11 Repeat Steps 2 through 10 to return the active/standby XTC cards to their configuration at the start of the procedure.

Step 12 Verify that the XTC cards appear as noted in Step 5.

Step 13 Return to your originating procedure (NTP).

DLP-B88 Optical 1+1 Protection Test

Purpose	This task verifies a 1+1 protection group will switch traffic properly.
Tools/Equipment	The test set specified by the acceptance test procedure.
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23; a test circuit created as part of the topology acceptance test.
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 From the View menu choose **Go to Network View**.

Step 2 Click the **Alarms** tab.

a. Verify that the network does not have any unexplained alarms. If unexplained alarms are present, resolve them before continuing. Refer to the *Cisco ONS 15327 Troubleshooting Guide*.

b. Ensure that the alarm filter icon in the lower right corner is not indented. If so, click it once to turn it off. When you are done checking for alarms, click the icon again to turn alarm filtering back on. See the "DLP-B227 Disable Alarm Filtering" task on page 6-29 for instructions.

Step 3 Click the **Conditions** tab. Verify that the network does not have any unexplained conditions. If unexplained conditions are present, resolve them before continuing. Refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 4 On the network may, double-click the node containing the 1+1 protection group you are testing.

Step 5 Click the **Maintenance > Protection** tabs.

Step 6 In the Protection Groups list, choose the 1+1 protection group.

Step 7 Click the working port. Next to Switch Commands, click the **Force** button.

Step 8 At the Confirm Manual Operation dialog, click **Yes**.

Step 9 Under Selected Group, verify that the following values appear:

Protect port - Protect/Active [FORCE_SWITCH_TO_PROTECT] [PORT STATE]

Working port - Working/Standby [FORCE_SWITCH_TO_PROTECT], [PORT STATE]

Step 10 Verify that traffic on the test set connected to the node is still running. Some bit errors are normal, but traffic flow should not be interrupted. If a traffic interruption occurs, complete Steps 11 and 12, then refer to your next level of support.

Step 11 Next to Switch Commands, click the **Clear** button.

Step 12 At the Confirm Clear Operation confirmation, click **Yes**.

Step 13 Under Selected Group, click the protect port. Next to Switch Commands, click the **Force** button.

Step 14 In the confirmation dialog box, click **Yes**.

Step 15 Under Selected Group, verify that the following values appear:

Protect port - Protect/Active [FORCE_SWITCH_TO_WORKING], [PORT STATE]

Working port - Working/Standby [FORCE_SWITCH_TO_WORKING], [PORT STATE]

Step 16 Verify that traffic on the test set connected to the node is still running. If a traffic interruption occurs, complete Steps 17 and 18, then refer to your next level of support.

Step 17 Next to Switch Commands, click the **Clear** button.

Step 18 In the Confirm Clear Operation dialog box, click **Yes**.

Step 19 Under Selected Group, verify the following states:

- Protect port - Protect/Standby
- Working port - Working/Active

Step 20 Return to your originating procedure (NTP).

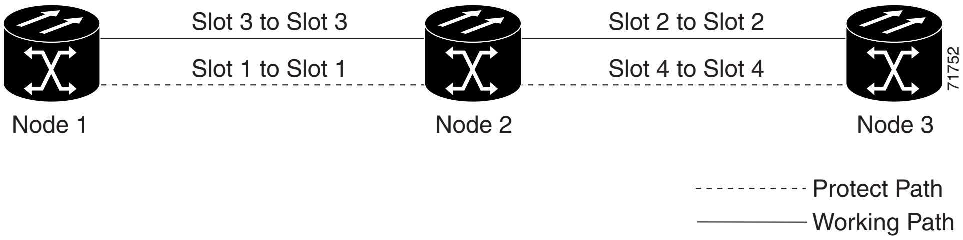
NTP-B38 Provision a Linear ADM Network

Purpose	This procedure provisions three or more ONS 15327s in a linear add-drop multiplexer (ADM) configuration.
Tools/Equipment	None
Prerequisite Procedures	NTP-B35 Verify Node Turn Up, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Log into an ONS 15327 that you want to provision in a linear ADM network. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. If you are already logged in, continue with Step 2.

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

Figure 4-1 Linear ADM Configuration



Step 2 Click the **Provisioning > Protection** tabs. Verify that 1+1 protection is created for the OC-N cards at the node. If the protection group has not been created, go to the "NTP-B170 Create Optical Protection Groups" procedure on page 3-20 to create them.

Step 3 Repeat Steps 1 and 2 for all other nodes you will include in the linear ADM.

Step 4 Verify that the working and protect cards in the 1+1 protection groups correspond to the physical fiber connections between the nodes, that is, working cards are fibered to working cards and protect cards are fibered to protect cards.

Step 5 Complete the "DLP-B253 Provision SONET DCC Terminations" task on page 4-4 for the working OC-N ports on each linear ADM node.

Note If linear ADM nodes are not connected to a LAN, you will need to create the DCC terminations using a craft (direct) connection to the node. Remote provisioning is possible only after all nodes that do not have LAN connections have DCC terminations provisioned to in-service OC-N ports.

Note Terminating nodes will have one DCC termination (Nodes 1 and 3 in Figure 4-1 on page 4-10), and intermediate nodes will have two DCC terminations (Node 2/Slot 3 and Node 2/Slot 2 in Figure 4-1).

Step 6 Verify that timing has been set up at each linear node. If not, complete the "NTP-B28 Set Up Timing" procedure on page 3-16. If a node is using line timing, use its working OC-N card as the timing source.

Step 7 Complete the "NTP-B174 Linear ADM Network Acceptance Test" procedure on page 4-11.

Stop. You have completed this procedure.

NTP-B174 Linear ADM Network Acceptance Test

Purpose	This procedure tests a linear ADM network.
Tools/Equipment	Test set/cables appropriate to the test circuit you will create
Prerequisite Procedures	NTP-B38 Provision a Linear ADM Network, page 4-10
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Log into an ONS 15327 on the linear ADM network you are testing. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. If you are already logged in, continue with Step 2.

Step 2 From the View menu choose **Go to Network View**.

Step 3 Click the **Alarms** tab.

a. Verify that the network does not have any unexplained alarms. If unexplained alarms are present, resolve them before continuing. Refer to the *Cisco ONS 15327 Troubleshooting Guide*.

b. Ensure that the alarm filter icon in the lower right corner is not indented. If so, click it once to turn it off. When you are done checking for alarms, click the icon again to turn alarm filtering back on. See the "DLP-B227 Disable Alarm Filtering" task on page 6-29 for instructions.

Step 4 Complete the "DLP-B139 Export CTC Data" task on page 6-3 to export alarm data to a file on your hard drive.

Step 5 Click the **Conditions** tab. Verify that the network does not have any unexplained conditions. If unexplained conditions are present, resolve them before continuing. Refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 6 Complete the "DLP-B139 Export CTC Data" task on page 6-3 to export condition data to a file on your hard drive.

Step 7 Display a linear ADM node in node view.

Step 8 Create a test circuit from that node to an adjacent linear ADM node.

- For DS-1 circuits, complete the "NTP-B181 Create an Automatically Routed DS-1 Circuit" procedure on page 5-5. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For DS-3 circuits, complete the "NTP-B184 Create an Automatically Routed DS-3 Circuit" procedure on page 5-16. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.

Step 9 Configure the test set for the test circuit type you created:

- DS-1—If you are testing an unmuxed DS-1, you must have a DSX-1 panel or a direct DS-1 interface into the ONS 15327 through the AMP Champ connectors on the MIC. Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- DS-3—If you are testing a clear channel DS-3, you must have a DSX-3 panel or a direct DS-3 interface into the ONS 15327 through the BNC connectors on the MIC. Set the test set for clear channel DS-3. For information about configuring your test set, consult your test set user guide.

Step 10 Verify the integrity of all patch cables that will be used in this test by connecting one end to the test set transmit (Tx) connector and the other end to the test set receive (Rx) connector. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before going to the next step.

Step 11 Create a physical loopback at the circuit destination card. To do so, attach one end of a patch cable to the destination port's transmit (Tx) connector; attach the other end to the destination port's receive (Rx) connector.

Step 12 At the circuit source card:

a. Connect the transmit (Tx) connector of the test set to the circuit receive (Rx) connector.

b. Connect the test set receive (Rx) connector to the circuit transmit (Tx) connector.

Step 13 Verify that the test set displays a clean signal. If a clean signal is not displayed, repeat Steps 8 through 12 to make sure the test set and cabling are configured correctly.

Step 14 Inject BIT errors from the test set. Verify that the errors appear on the test set, indicating a complete end-to-end circuit.

Step 15 Complete the "DLP-B254 XTC Active/Standby Switch Test" task on page 4-7.

Step 16 Complete the "DLP-B88 Optical 1+1 Protection Test" task on page 4-8 to test the OC-N port protection group switching.

Step 17 Set up and complete a BER test. Use the existing configuration and follow your site requirements for length of time. Record the test results and configuration.

Step 18 Remove any loopbacks, switches, or test sets from the nodes after all testing is complete. Refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 19 Click the **Alarms** tab. Verify that the network does not have any unexplained alarms. If unexplained alarms are present, resolve them before continuing. Refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 20 Delete the test circuit. See the "NTP-B152 Delete Circuits" procedure on page 8-13 for instructions.

Step 21 Display the next linear ADM node in node view and repeat Steps 8 through 20.

Step 22 If a node fails any test, repeat the test while verifying correct setup and configuration. If the test fails again, refer to the next level of support.

After all tests are successfully completed and no alarms exist in the network, the network is ready for service application.

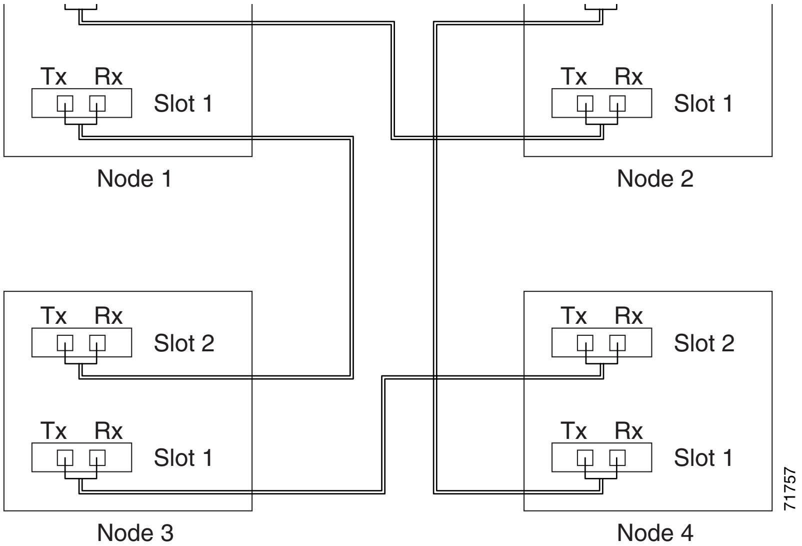
Stop. You have completed this procedure.

NTP-B40 Provision BLSR Nodes

Purpose	This procedure provisions ONS 15327 nodes for a bidirectional line switched ring.
Tools/Equipment	None
Prerequisite Procedures	NTP-B35 Verify Node Turn Up, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B44 Install Fiber-Optic Cables for BLSR Configurations" task on page 1-46, verifying that the east port at one node is connected to the west port on an adjacent node, and this east to west port connection is used at all BLSR nodes, similar to Figure 4-2. In the figure, the OC-N drop card on the left side of the shelf is the west port, and the drop card on the right side of the shelf is the east port.

Figure 4-2 Four-Node, Two-Fiber BLSR Fiber Connection Example



Step 2 Log into an ONS 15327 that you want to configure in a BLSR. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. If you are already logged in, continue with Step 3.

Step 3 Complete the "DLP-B253 Provision SONET DCC Terminations" task on page 4-4. Provision the two ports/cards that will serve as the BLSR ports at the node.

Note If an ONS 15327 is not connected to a corporate LAN, DCC provisioning must be performed through a craft (direct) connection to the node. Remote provisioning is possible only after all nodes in the network have DCC provisioned to in-service OC-N ports.

Step 4 Repeat Steps 2 and 3 at each node that will be in the BLSR. Verify that the EOC (DCC Termination Failure) and LOS (Loss of Signal) alarms are clear after you provision all the DCCs in the ring.

Step 5 Complete the "NTP-B126 Create a BLSR" procedure on page 4-14.

Stop. You have completed this procedure.

NTP-B126 Create a BLSR

Purpose	This procedure creates a BLSR at each BLSR-provisioned node.
Tools/Equipment	None
Prerequisite Procedures	NTP-B35 Verify Node Turn Up, page 4-2 NTP-B40 Provision BLSR Nodes, page 4-13
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into an ONS 15327 node on the network where you will create the BLSR. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. If you are already logged in, continue with Step 2.

Step 2 From the View menu choose **Go to Network View**.

Step 3 Click the **Provisioning > BLSR** tabs.

Step 4 Click **Create BLSR**.

Step 5 On the BLSR Creation dialog box (Figure 4-3), set the BLSR properties:

- Ring Type—Choose the BLSR ring type, either two-fiber or four-fiber.
- Speed—Choose the BLSR ring speed: OC-12 or OC-48. The speed must match the OC-N speed of the BLSR trunk (span) cards.
- Ring ID—Assign a ring ID (a number between 0 and 9999).
- Reversion time—Set the amount of time that will pass before the traffic reverts to the original working path following a ring switch. The default is 5 minutes. Ring reversions can be set to Never.

Figure 4-3 Setting BLSR Properties

Step 6 Click **Next**. If CTC displays a network graphic, go to Step 7. If CTC determines that a BLSR cannot be created, for example, not enough optical cards are installed or it finds circuits with UPSR selectors, a "Cannot Create BLSR" message appears. If this occurs, complete the following steps:

a. Click **OK**.

b. On the Create BLSR window, click **Excluded Nodes**. Review the information explaining why the BLSR could not be created, then click **OK**.

c. Depending on the problem, click **Back** to start over or click **Cancel** to cancel the operation.

d. Complete the "NTP-B40 Provision BLSR Nodes" procedure on page 4-13, making sure all steps are completed accurately, then start this procedure again.

Step 7 In the network graphic, double-click a BLSR span line. If the span line is DCC connected to other BLSR cards comprising a complete ring, the lines turn blue and the **Finish** button appears. If the lines do not form a complete ring, double-click span lines until a complete ring is formed. When the ring is DCC connected, go to Step 8.

Step 8 Click **Finish**. If CTC displays the BLSR window with the BLSR you created, go to Step 9. If CTC displays a "Cannot Create BLSR" or "Error While Creating BLSR" message:

a. Click **OK**.

b. On the Create BLSR window, click **Excluded Nodes.** Review the information explaining why the BLSR could not be created, then click **OK**.

c. Depending on the problem, click **Back** to start over or click **Cancel** to cancel the operation.

d. Complete the "NTP-B40 Provision BLSR Nodes" procedure on page 4-13, making sure all steps are completed accurately, then start this procedure again.

Note Some or all of the following alarms may briefly appear during BLSR setup: E-W MISMATCH, RING MISMATCH, APSCIMP, APSDFLTK, or BLSROSYNC.

Step 9 Verify the following:

- On the network view graphic, a green span line appears between all BLSR nodes.
- All E-W MISMATCH, RING MISMATCH, APSCIMP, DFLTK, and BLSROSYNC alarms are cleared. See the *Cisco ONS 15327 Troubleshooting Guide* for alarm troubleshooting.

Step 10 Complete the "NTP-B175 BLSR Acceptance Test" procedure on page 4-16.

Stop. You have completed this procedure.

NTP-B175 BLSR Acceptance Test

Purpose	This procedure tests a two-fiber BLSR.
Tools/Equipment	Test set and cables appropriate for the test circuit
Prerequisite Procedures	NTP-B40 Provision BLSR Nodes, page 4-13 NTP-B126 Create a BLSR, page 4-14
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note This procedure requires that you create test circuits and perform span switches around the ring. For clarity, "Node 1" refers to the login node where you begin the procedure. "Node 2" refers to the node connected to the east OC-N trunk (span) card of Node 1, "Node 3" refers to the node connected to the east OC-N trunk card of Node 2, and so on.

Step 1 Log into one of the ONS 15327s on the BLSR you are testing. (This node will be called Node 1.) See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. If you are already logged in, continue with Step 2.

Step 2 From the View menu choose **Go to Network View**.

Step 3 Click the **Alarms** tab.

- **a.** Verify that the network does not have any unexplained alarms. If unexplained alarms are present, resolve them before continuing. Refer to the *Cisco ONS 15327 Troubleshooting Guide*.
- **b.** Ensure that the alarm filter icon in the lower right corner is not indented. If so, click it once to turn it off. When you are done checking for alarms, click the icon again to turn alarm filtering back on. See the "DLP-B227 Disable Alarm Filtering" task on page 6-29 for instructions.

Step 4 Complete the "DLP-B139 Export CTC Data" task on page 6-3 to export alarm data to a file on your hard drive.

Step 5 Click the **Conditions** tab. Verify that the network does not have any unexplained conditions. If unexplained conditions are present, resolve them before continuing. Refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 6 Complete the "DLP-B139 Export CTC Data" task on page 6-3 to export condition data to a file on your hard drive.

Step 7 On the network view, double-click Node 1.

Step 8 Complete the "DLP-B217 BLSR Exercise Ring Test" task on page 4-18.

Step 9 Create a test circuit from Node 1 to the node connected to the east OC-N trunk card of Node 1. (This node will be called Node 2.)

- For DS-1 circuits, complete the "NTP-B181 Create an Automatically Routed DS-1 Circuit" procedure on page 5-5. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For DS-3 circuits, complete the "NTP-B184 Create an Automatically Routed DS-3 Circuit" procedure on page 5-16. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.

Step 10 Configure the test set for the test circuit type you created:

- DS-1—If you are testing an unmuxed DS-1, you must have a DSX-1 panel or a direct DS-1 interface into the ONS 15327 through the AMP Champ connectors on the MIC. Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- DS-3—If you are testing a clear channel DS-3, you must have a DSX-3 panel or a direct DS-3 interface into the ONS 15327 through the BNC connectors on the MIC. Set the test set for clear channel DS-3. For information about configuring your test set, consult your test set user guide.

Step 11 Verify the integrity of all patch cables that will be used in this test by connecting the test set transmit (Tx) connector to the test set receive (Rx) connector. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before going to the next step.

Step 12 Create a physical loopback at the circuit destination card: attach one end of a patch cable to the destination port transmit (Tx) connector; attach the other end to the port receive (Rx) connector.

Step 13 At the circuit source card:

a. Connect the transmit (Tx) connector of the test set to the circuit receive (Rx) connector.

b. Connect the test set receive (Rx) connector to the circuit transmit (Tx) connector.

Step 14 Verify that the test set displays a clean signal. If a clean signal is not displayed, repeat Steps 9 through 13 to make sure the test set and cabling are configured correctly.

Step 15 Inject BIT errors from the test set. Verify that the errors display at the test set, verifying a complete end-to-end circuit.

Step 16 Complete the "DLP-B254 XTC Active/Standby Switch Test" task on page 4-7.

Step 17 Complete the "DLP-B91 BLSR Ring Switch Test" task on page 4-19 at Node 1.

Step 18 Set up and complete a BER test on the test circuit. Use the existing configuration and follow your site requirements for length of time. Record the test results and configuration.

Step 19 Complete the "NTP-B152 Delete Circuits" procedure on page 8-13 for the test circuit.

Step 20 Repeating Steps 7 through 19 for Nodes 2 and higher, work your way around the BLSR, testing each node and span in the ring. Work your way around the BLSR creating test circuits between every two consecutive nodes.

Step 21 After you test the entire ring, remove any loopbacks and test sets from the nodes.

Step 22 If a node fails any test, repeat the test while verifying correct setup and configuration. If the test fails again, refer to the next level of support.

After all tests are successfully completed and no alarms exist in the network, the network is ready for service application. Continue with Chapter 5, "Create Circuits and VT Tunnels."

Stop. You have completed this procedure.

DLP-B217 BLSR Exercise Ring Test

Purpose	This task tests the BLSR functionality without switching traffic. Ring exercise conditions are reported and cleared within 10 to 15 seconds.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 From the View menu choose **Go to Network View**.

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

Step 3 Click the row of the BLSR you will exercise, then click **Edit**.

Step 4 Right-click the west port of any BLSR node and choose **Set West Protection Operation**. (To move a graphic icon, press **Ctrl** while you drag and drop it to a new location.)

Note For two-fiber BLSRs, the squares on the node icons represent the BLSR working and protect channels. You can right-click either channel.

Step 5 On the Set West Protection Operation dialog box, choose **EXERCISE RING** from the drop-down menu. Click **OK**.

Step 6 On the Confirm BLSR Operation dialog box, click **Yes**.

On the network view graphic, an E appears on the BLSR channel where you invoked the exercise. The E will display for 10 to 15 seconds, then disappear.

Step 7 In the CTC window, click the **History** tab. Verify that the node where you exercised the ring has an EXERCISE-RING (Exercising Ring Successfully) condition appear. Other conditions displayed include EXERCISE-RING-REQ and FE-EXERCISING-RING.

If you do not see any BLSR exercise conditions, click the **Filter** button and verify that filtering is not turned on. Also, check that alarms and conditions are not suppressed for a node or BLSR trunk cards. See the "NTP-B72 Suppress and Discontinue Alarm Suppression" procedure on page 6-29 for more information.

Step 8 Click the **Alarms** tab. Verify that the network does not have any unexplained alarms. If unexplained alarms are present, resolve them before continuing. Refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 9 From the File menu choose **Close** to close the BLSR window.

Step 10 Return to your originating procedure (NTP).

DLP-B91 BLSR Ring Switch Test

Purpose	This task verifies that protection switching is working correctly in a BLSR.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In the network view click the **Provisioning > BLSR** tabs.

Step 2 Click the row of the BLSR you will switch, then click **Edit**.

Step 3 Right-click any BLSR node west port and choose **Set West Protection Operation**. (To move a graphic icon, click it, then press **Ctrl** while you drag and drop it to a new location.)

Note The squares on the node icons represent the BLSR working and protect channels. You can right-click either channel.

Step 4 On the Set West Protection Operation dialog box, choose **FORCE RING** from the drop-down menu. Click **OK**.

Step 5 Click **Yes** on the two Confirm BLSR Operation dialog boxes that appear.

On the network view graphic, an F appears on the working BLSR channel where you invoked the Force Ring switch. The BLSR span lines turn purple where the Force was invoked, and all span lines between other BLSR nodes turn green.

Step 6 Click the **Conditions** tab, then click **Retrieve**.

Step 7 Verify that the following conditions are reported on the node where you invoked the Force switch on the west port:

- FORCE-REQ-RING—A Force Switch Request On Ring condition is reported against the span's working slot on the west side of the node.
- RING-SW-EAST—A Ring Switch Active on the east side condition is reported against the working span on the east side of the node.

Note Make sure the Filter button in the lower right corner of the window is off. Click the Node column to sort conditions by node.

Step 8 Verify that the following conditions are reported on the node that is connected to the west line of the node where you performed the switch:

- FE-FRCDWKSWPR-RING—A Far-End Working Facility Forced to Switch to Protection condition is reported against the working span on the east side of the node.
- RING-SW-WEST—A Ring Switch Active on the west side condition is reported against the working span on the west side of the node.

Step 9 Verify the BLSR line status on each node:

a. In node view, click **Maintenance** > **BLSR**.

b. Verify the following:

- The line states are shown as Stby/Stby on the west side of the node and Act/Act on the east side of the node where you invoked the Force Ring switch.
- The line states are shown as Stby/Stby on the east side of the node and Act/Act on the west side of the node that is connected to the west line of the node where you invoked the Force Ring switch.
- The line states are shown as Act/Act on both East and west sides of the remaining nodes in the ring.

Step 10 From network view, click the **Alarms** tab.

a. Verify that the network does not have any unexplained alarms. If unexplained alarms are present, resolve them before continuing. Refer to the *Cisco ONS 15327 Troubleshooting Guide.*

b. Ensure that the alarm filter icon in the lower right corner is not indented. If so, click it once to turn it off. When you are done checking for alarms, click the icon again to turn alarm filtering back on. See the "DLP-B227 Disable Alarm Filtering" task on page 6-29 for instructions.

Step 11 Display the BLSR window where you invoked the Force Ring switch (the window may be hidden by the CTC window).

Step 12 Right-click the west port of the BLSR node where you invoked the Force Ring switch and choose **Set West Protection Operation**.

Step 13 On the Set West Protection Operation dialog box, choose **CLEAR** from the drop-down menu. Click **OK**.

Step 14 Click **Yes** on the Confirm BLSR Operation dialog box.

On the network view graphic, the Force Ring switch is removed, the F indicating the switch is removed, and the span lines between BLSR nodes are purple and green. The span lines may take a few moments to change color.

Step 15 From network view, click the **Conditions** tab. Verify that all conditions raised in this procedure are cleared from the network. If unexplained conditions are present, resolve them before continuing.

Step 16 Verify the BLSR line status on each node:

a. From node view, click **Maintenance** > **BLSR**.

b. Verify that the line states are shown as Act/Stby on both the East and west sides of each node in the ring.

Step 17 Right-click the east port of BLSR node and choose **Set East Protection Operation**.

Step 18 On the Set East Protection Operation dialog box, choose **FORCE RING** from the drop-down menu. Click **OK**.

Step 19 Click **Yes** on the two Confirm BLSR Operation dialog boxes that appear.

On the network view graphic, an F appears on the working BLSR channel where you invoked the Force Ring switch. The BLSR span lines are purple where the Force was invoked, and all span lines between other BLSR nodes are green. The span lines may take a few moments to change color.

Step 20 Click the **Conditions** tab, then click **Retrieve**.

Step 21 Verify that the following conditions are reported on the node where you invoked the Force Ring switch on the east port:

- FORCE-REQ-RING—A Force Switch Request On Ring condition is reported against the working span on the east side of the node.
- RING-SW-WEST—A Ring Switch Active on the west side condition is reported against the working span on the east side of the node.

Note Make sure the **Filter** button in the lower right corner of the window is off. Click the Node column to sort conditions by node.

Step 22 Verify that the following conditions are reported on the node that is connected via the east line to the node where you performed the switch:

- FE-FRCDWKSWPR-RING—A Far-End Working Facility Forced to Switch to Protection condition is reported against the working span on the west side of the node.
- RING-SW-EAST—A Ring Switch Active on the east side condition is reported against the working span on the west side of the node.

Step 23 Verify the BLSR line status on each node:

a. From node view, click **Maintenance** > **BLSR**.

b. Verify the following:

- The line states are shown as Stby/Stby on the east side of the node and Act/Act on the west side of the node where you invoked the Force Ring switch.
- The line states are shown as Stby/Stby on the west side of the node and Act/Act on the east side of the node that is connected to the east line of the node where you invoked the Force Ring switch.
- The line states are shown as Act/Act on both East and west sides of the remaining nodes in the ring.

Step 24 From network view, click the **Alarms** tab. Verify that the network does not have any unexplained alarms. If unexplained alarms are present, resolve them before continuing. Refer to the *Cisco ONS 15327 Troubleshooting Guide.*

Step 25 Display the BLSR window where you invoked the Force Ring switch (the window may be hidden by the CTC window).

Step 26 Right-click the west port of the BLSR node where you invoked the Force Ring switch and choose **Set East Protection Operation**.

Step 27 On the Set East Protection Operation dialog box, choose **CLEAR** from the drop-down menu. Click **OK**.

Step 28 Click **Yes** on the Confirm BLSR Operation dialog box.

On the network view graphic, the Force Ring switch is removed, the F indicating the switch is removed, and the span lines between BLSR nodes will be purple and green. The span lines may take a few moments to change color.

Step 29 From network view, click the **Conditions** tab. Verify that all conditions raised in this procedure are cleared from the network. If unexplained conditions are present, resolve them before continuing.

Step 30 Verify the BLSR line status on each node:

a. From node view, click **Maintenance** > **BLSR**.

b. Verify that the line states are shown as Act/Stby on both the East and west sides of each node in the ring.

Step 31 From the File menu choose **Close** to close the BLSR window.

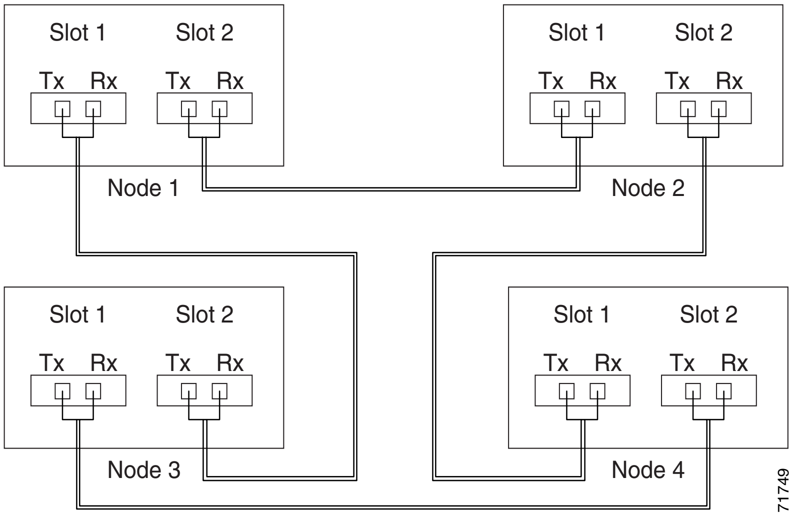
Step 32 Return to your originating procedure (NTP).

NTP-B44 Provision UPSR Nodes

Purpose	This procedure provisions nodes for inclusion in a unidirectional path switched ring (UPSR). A UPSR is created after the fiber connections are made.
Tools/Equipment	None
Prerequisite Procedures	NTP-B35 Verify Node Turn Up, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Verify that the fiber is correctly connected to the UPSR trunk (span) OC-N cards similar to Figure 4-4.

Figure 4-4 UPSR Fiber Connection Example



Step 2 Log into an ONS 15327 in the UPSR you are turning up. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. If you are already logged in, continue with Step 3.

Step 3 Complete the "DLP-B253 Provision SONET DCC Terminations" task on page 4-4 for the two cards/ports that will serve as the UPSR ports on the node, for example, Slot 2 (OC-48)/Node 1 and Slot 1 (OC-48)/ Node 1.

Note If an ONS 15327 is not connected to a corporate LAN, DCC provisioning must be performed through a craft (direct) connection. Remote provisioning is possible only after all nodes in the network have DCC terminations provisioned to in-service OC-N ports.

Step 4 Repeat Steps 2 and 3 for each node in the UPSR.

Step 5 Complete the "NTP-B177 UPSR Acceptance Test" procedure on page 4-23.

Stop. You have completed this procedure.

NTP-B177 UPSR Acceptance Test

Purpose	This procedure tests a UPSR.
Tools/Equipment	Test set and cables appropriate to the test circuit you will create
Prerequisite Procedures	NTP-B44 Provision UPSR Nodes, page 4-22
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

Step 2 From the View menu choose **Go to Network View**.

Step 3 Click the **Alarms** tab.

a. Verify that the network does not have any unexplained alarms. If unexplained alarms are present, resolve them before continuing. Refer to the *Cisco ONS 15327 Troubleshooting Guide*.

b. Ensure that the alarm filter icon in the lower right corner is not indented. If so, click it once to turn it off. When you are done checking for alarms, click the icon again to turn alarm filtering back on. See the "DLP-B227 Disable Alarm Filtering" task on page 6-29 for instructions.

Step 4 Complete the "DLP-B139 Export CTC Data" task on page 6-3 to export alarm data to a file on your hard drive.

Step 5 Click the **Conditions** tab. Verify that the network does not have any unexplained conditions. If unexplained conditions are present, resolve them before continuing. Refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 6 Complete the "DLP-B139 Export CTC Data" task on page 6-3 to export condition data to a file on your hard drive.

Step 7 On the network map, double-click the node that you logged into in Step 1.

Step 8 Create a test circuit from that node to the next adjacent UPSR node.

- For DS-1 circuits, complete the "NTP-B181 Create an Automatically Routed DS-1 Circuit" procedure on page 5-5. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.
- For DS-3 circuits, complete the "NTP-B184 Create an Automatically Routed DS-3 Circuit" procedure on page 5-16. When you set the circuit state, choose **IS** and check the **Apply to drop ports** check box.

Step 9 Configure the test set for the test circuit type you created:

- DS-1—If you are testing an unmuxed DS-1, you must have a DSX-1 panel or a direct DS-1 interface into the ONS 15327 through the AMP Champ connectors on the MIC. Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- DS-3—If you are testing a clear channel DS-3, you must have a DSX-3 panel or a direct DS-3 interface into the ONS 15327 through the BNC connectors on the MIC. Set the test set for clear channel DS-3. For information about configuring your test set, consult your test set user guide.

Step 10 Verify the integrity of all patch cables that will be used in this test by connecting one end to the test set transmit (Tx) connector and the other end to the test set receive (Rx) connector. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before continuing.

Step 11 Create a physical loopback at the circuit destination card:

a. Attach one end of a patch cable to the destination port transmit (Tx) connector.

b. Attach the other end to the port receive (Rx) connector.

Step 12 At the circuit source card:

a. Connect the transmit (Tx) connector of the test set to the circuit receive (Rx) connector.

b. Connect the test set receive (Rx) connector to the circuit transmit (Tx) connector.

Step 13 Verify that the test set displays a clean signal. If a clean signal is not displayed, repeat Steps 1 through 10 to make sure the test set and cabling are configured correctly.

Step 14 Inject BIT errors from the test set. To verify that you have a complete end-to-end circuit, verify that the errors display at the test set.

Step 15 Complete the "DLP-B254 XTC Active/Standby Switch Test" task on page 4-7.

Step 16 From the View menu choose **Go to Network View**.

Step 17 Click one of the two spans leaving the circuit source node and complete the "DLP-B94 UPSR Protection Switching Test" task on page 4-25 for instructions.

Although a service interruption under 60 ms may occur, the test circuit should continue to work before, during, and after the switches. If the circuit stops working, do not continue. Contact your next level of support.

Step 18 In network view, click the other circuit source span and complete the "DLP-B94 UPSR Protection Switching Test" task on page 4-25 for instructions.

Although a service interruption under 60 ms may occur, the test circuit should continue to work before, during, and after the switches. If the circuit stops working, do not continue. Contact your next level of support.

Step 19 Set up and complete a BER Test. Use the existing configuration and follow your site requirements for the length of time. Record the test results and configuration.

Step 20 Complete the "NTP-B152 Delete Circuits" procedure on page 8-13 for the test circuit.

Step 21 Remove any loopbacks, switches, or test sets from the nodes after all testing is complete. Refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 22 View the alarms and conditions on each node and record results by exporting them to a file. See the "DLP-B139 Export CTC Data" task on page 6-3 for instructions.

Step 23 Repeat Steps 8 through 22 for each node on the network.

Step 24 If a node fails any test, repeat the test while verifying correct setup and configuration. If the test fails again, refer to the next level of support.

After all tests are successfully completed and no alarms exist in the network, the network is ready for service application. Continue with Chapter 5, "Create Circuits and VT Tunnels."

Stop. You have completed this procedure.

DLP-B94 UPSR Protection Switching Test

Purpose	This task verifies that a UPSR span is switching correctly.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 From the View menu choose **Go to the Network View**.

Step 2 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box displays the UPSR circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 3 Click the **Perform UPSR span switching** field and choose **FORCE SWITCH AWAY** from the drop-down menu. Click **Apply**.

Step 4 In the Confirm UPSR Switch dialog box, click **Yes**.

Step 5 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span dialog box, the Switch State for all circuits is Force. Unprotected circuits will not switch.

Step 6 Click the **Perform UPSR span switching** field and choose **CLEAR** from the drop-down menu. Click **Apply**. Click **Yes** to confirm.

Step 7 In the Confirm UPSR Switch dialog box, click **Yes**.

Step 8 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span window, the Switch State for all UPSR circuits is CLEAR.

Step 9 Return to your originating procedure (NTP).

NTP-B46 Subtend a UPSR from a BLSR

Purpose	This procedure subtends a UPSR from an existing BLSR.
Tools/Equipment	One BLSR node must have OC-N cards and fibers to carry the UPSR.
Prerequisite Procedures	NTP-B175 BLSR Acceptance Test, page 4-16
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In the node that will subtend the UPSR (Node 3 in Figure 4-5), install the two (east/west) OC-N cards that will serve as the UPSR trunk (span) cards (Node 3, Slots 3 and 4). See the "NTP-B218 Install the Optical and Ethernet Cards" procedure on page 1-23. If they are already installed, go to Step 2.

Step 2 Attach fibers from these cards to the UPSR trunk cards on the neighbor UPSR node or nodes.

Step 3 Log into the ONS 15327 that will subtend the UPSR. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions.

Step 4 Complete the "DLP-B253 Provision SONET DCC Terminations" task on page 4-4 for each OC-N card that will carry the UPSR.

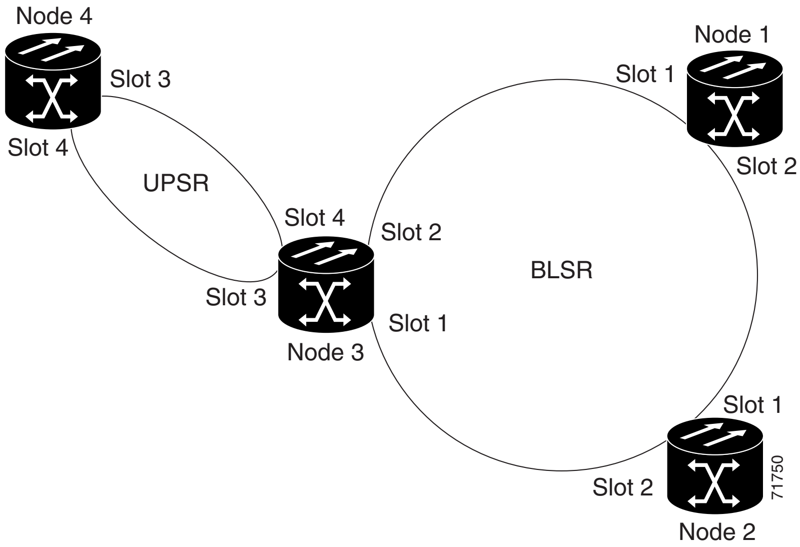
Step 5 Log into the UPSR node that connects to the node in Step 3.

Step 6 Complete the "DLP-B253 Provision SONET DCC Terminations" task on page 4-4 for each OC-N card that will carry the UPSR.

Step 7 Repeat Step 6 for each node in the UPSR.

Step 8 From the View menu choose **Go To Network View**.

Figure 4-5 UPSR Subtended from a BLSR



Step 9 Complete the "NTP-B177 UPSR Acceptance Test" procedure on page 4-23.

Stop. You have completed this procedure.

NTP-B47 Subtend a BLSR from a UPSR

Purpose	This procedure subtends a BLSR from an existing UPSR.
Tools/Equipment	One UPSR node must have OC-N cards and fibers to carry the BLSR.
Prerequisite Procedures	NTP-B177 UPSR Acceptance Test, page 4-23
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In the UPSR node that will subtend the BLSR, install the two (east and west) OC-N cards that will serve as the BLSR trunk (span) cards (in Figure 4-5 on page 4-26, Node 3, Slots 1 and 2). See the "NTP-B218 Install the Optical and Ethernet Cards" procedure on page 1-23.

Step 2 Attach fibers from the cards in Step 1 to the BLSR trunk cards on another BLSR node or nodes. In Figure 4-5 on page 4-26, Slot 1/Node 3 connects to Slot 2/Node 2, and Slot 2/Node 3 connects to Slot 1/Node 1.

Step 3 Log into the ONS 15327 that will subtend the BLSR (the node in Step 1). See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. If you are already logged in, continue with Step 4.

Step 4 Create the DCCs on both OC-N trunk cards (east and west) that will carry the BLSR. See the "DLP-B253 Provision SONET DCC Terminations" task on page 4-4 for instructions.

Step 5 Create the subtending BLSR:

a. Complete the "NTP-B40 Provision BLSR Nodes" procedure on page 4-13 for each node that will be in the BLSR. If you have already provisioned the BLSR, perform this procedure for the subtending node only.

b. Complete the "NTP-B126 Create a BLSR" procedure on page 4-14. Include the node in Step 3 (the node that will subtend the BLSR) in the BLSR.

Step 6 From the View menu choose **Go to the Network View** to see the subtending ring.

Stop. You have completed this procedure.

NTP-B48 Subtend a BLSR from a BLSR

Purpose	This procedure subtends a BLSR from an existing BLSR.
Tools/Equipment	One BLSR node must have OC-N cards and fibers needed to carry the second BLSR.
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note This procedure assumes that all nodes are configured for the BLSR. If you need to add a node to a BLSR, see the "NTP-B12 Add a BLSR Node" procedure on page 13-2.

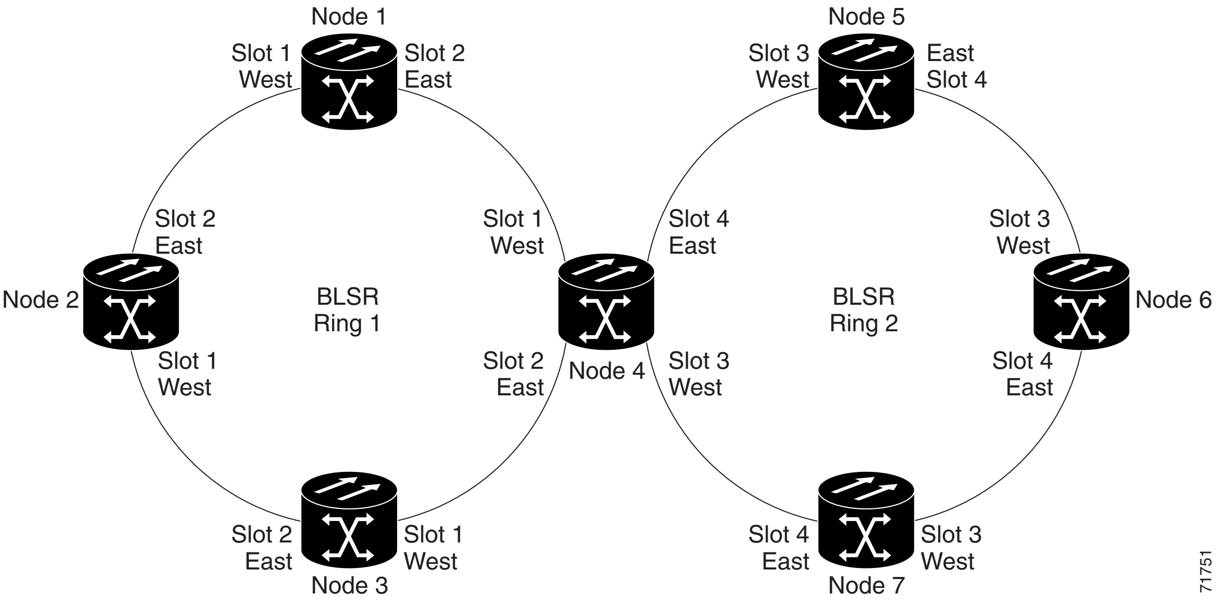
Step 1 Log into the node that will subtend the BLSR. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. If you are already logged in, continue with Step 2.

Step 2 Install the OC-N cards that will serve as the BLSR trunk (span) cards if they are not already installed. See the "NTP-B218 Install the Optical and Ethernet Cards" procedure on page 1-23.

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

Note Although different node IDs are used for the two BLSRs shown in Figure 4-6, nodes in different BLSRs can use the same node ID.

Figure 4-6 BLSR Subtended from a BLSR



Step 3 Attach fibers from the trunk cards in the subtending node to the BLSR trunk cards on its two neighboring BLSR nodes. In Figure 4-6, Node 4/Slot 3 connects to Node 7/Slot 4, and Node 4/Slot 4 connects to Node 5/Slot 3.

Step 4 Create the DCCs on the first OC-N card that will carry the BLSR. See the "DLP-B253 Provision SONET DCC Terminations" task on page 4-4 for instructions.

Step 5 Repeat Step 4 for the second OC-N trunk card that will carry the BLSR.

Step 6 Complete the "NTP-B40 Provision BLSR Nodes" procedure on page 4-13 for each node that will be in the BLSR. If you have already provisioned the BLSR, perform this procedure for the subtending node only.

Step 7 If the subtending BLSR is not already created, complete the "NTP-B126 Create a BLSR" procedure on page 4-14 to provision the new BLSR. The subtending BLSR must have a ring ID that differs from the ring ID of the first BLSR. The subtending node can have one Node ID that is used in both BLSRs, or a different Node ID for each BLSR. For example, the same node can be Node 4 in BLSR 1 and Node 2 in BLSR 2.

Step 8 Display the network view to see the subtending ring.

Step 9 Complete the "NTP-B175 BLSR Acceptance Test" procedure on page 4-16.

Stop. You have completed this procedure.

CHAPTER 5

Create Circuits and VT Tunnels

This chapter explains how to create Cisco ONS 15327 electrical circuits, VT tunnels, optical circuits, and Ethernet circuits. For additional information about ONS 15327 circuits, refer to the Circuits and Tunnels chapter in the *Cisco ONS 15327 Reference Manual*.

Before You Begin

Before performing any of the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15327 Troubleshooting Guide* as necessary.

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-B127 Verify Network Turn Up, page 5-3—Complete this procedure before you create any circuits.
2. NTP-B181 Create an Automatically Routed DS-1 Circuit, page 5-5—Complete as needed.
3. NTP-B182 Create a Manually Routed DS-1 Circuit, page 5-9—Complete as needed.
4. NTP-B183 Create a Unidirectional DS-1 Circuit with Multiple Drops, page 5-11—Complete as needed.
5. NTP-B184 Create an Automatically Routed DS-3 Circuit, page 5-16—Complete as needed.
6. NTP-B185 Create a Manually Routed DS-3 Circuit, page 5-20—Complete as needed.
7. NTP-B186 Create a Unidirectional DS-3 Circuit with Multiple Drops, page 5-22—Complete as needed.
8. NTP-B133 Create an Automatically Routed VT Tunnel, page 5-28—Complete as needed.
9. NTP-B134 Create a Manually Routed VT Tunnel, page 5-30—Complete as needed.
10. NTP-B135 Test Electrical Circuits, page 5-33—Complete this procedure after you create an electrical circuit.
11. NTP-B188 Create an Automatically Routed Optical Circuit, page 5-35—Complete as needed.
12. NTP-B189 Create a Manually Routed Optical Circuit, page 5-38—Complete as needed.
13. NTP-B190 Create a Unidirectional Optical Circuit with Multiple Drops, page 5-41—Complete as needed.
14. NTP-B62 Test Optical Circuits, page 5-46—Complete this procedure after you create an optical circuit.
15. NTP-B191 Create an E-Series EtherSwitch Circuit (Multicard or Single-Card Mode), page 5-48—Complete as needed.

16. NTP-B192 Create a Circuit for an E-Series Card in Port-Mapped Mode, page 5-50—Complete as needed.
17. NTP-B142 Create an E-Series Shared Packet Ring Ethernet Circuit, page 5-52—Complete as needed.
18. NTP-B143 Create an E-Series Hub and Spoke Ethernet Configuration, page 5-55—Complete as needed.
19. NTP-B144 Create an E-Series Single-Card EtherSwitch Manual Cross-Connect, page 5-57—Complete as needed.
20. NTP-B145 Create an E-Series Multicard EtherSwitch Manual Cross-Connect, page 5-60—Complete as needed.
21. NTP-B146 Test E-Series Circuits, page 5-67—Complete this procedure after you create E-Series SONET circuits.
22. NTP-B147 Create a G-Series Circuit, page 5-68—Complete as needed.
23. NTP-B148 Create a Manual Cross-Connect for a G-Series or an E-Series in Port-Mapped Mode, page 5-70—Complete as needed.
24. NTP-B149 Test G-Series Circuits, page 5-73—Complete this procedure after you create G-Series SONET circuits.

Table 5-1 defines ONS 15327 circuit creation terms and options.

Table 5-1 ONS 15327 Circuit Options

Circuit Option	Description
Source	The circuit source is where the circuit enters the ONS 15327 network.
Destination	The circuit destination is where the circuit exits an ONS 15327 network.
Automatic circuit routing	CTC routes the circuit automatically on the shortest available path based on routing parameters and bandwidth availability.
Manual circuit routing	Manual routing allows you to choose a specific path, not just the shortest path chosen by automatic routing. You can choose a specific STS or VT for each circuit segment and create circuits from work orders prepared by an operations support system (OSS) like the Telcordia TIRKS system.
VT tunnel	VT tunnels allow VT1.5 circuits to pass through an ONS 15327 without utilizing cross-connect resources. VT circuits using VT tunnels will use cross-connect capacity only at the source and destination nodes. One VT tunnel can carry 28 VT1.5 circuits.
VT Aggregation Point	VT aggregation points (VAPs) allow VT circuits to be aggregated into an STS to reduce VT matrix resource utilization. The STS grooming end of the VAP requires an OC-N card.

ONS 15327 circuits are either VT or STS circuits. Table 5-2 shows the circuit source and destination options for VT circuits.

Table 5-2 CTC Circuit Source and Destination Options For VT Circuits

Card	Ports	STSs	VTs	DS1s	DS3s
XTC-14	–	–	–	14	–
XTC-28-3	–	–	–	28	3

Table 5-2 CTC Circuit Source and Destination Options For VT Circuits (continued)

Card	Ports	STSs	VTs	DS1s	DS3s
OC3 IR 4 1310	4	3 per port	28 per STS	–	–
OC12 IR 1310 OC12 LR 1550	–	12	28 per STS	–	–
OC48 IR 1310 OC48 LR 1550	–	48	28 per STS	–	–

Table 5-3 shows the options that display for STS circuits.

Table 5-3 CTC Circuit Source and Destination Options for STS Circuits

Card	Ports	STSs	DS1s	DS3s
XTC-14	–	–	–	–
XTC-28-3	4	–	1	3
OC3 IR 4 1310	1	3 per port	–	–
OC12 IR 1310 OC12 LR 1550	1	12	–	–
OC48 IR 1310 OC48 LR 1550	–	48	–	–

NTP-B127 Verify Network Turn Up

Purpose	This procedure verifies that the ONS 15327 network is ready for circuit provisioning.
Tools/Equipment	None
Prerequisite Procedures	Chapter 4, “Turn Up Network”
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the “DLP-B60 Log into CTC” task on page 2-23 at an ONS 15327 on the network where you will create circuits. If you are already logged in, continue with Step 2.

Step 2 From the View menu choose **Go to Network View**. Wait for all the nodes that are part of the network to appear on the network map. (Large networks may take several minutes to display all the nodes.)

Note If this is the first time your computer has connected to this ONS 15327 network, the node icons will be stacked on the left side of the graphic area, possibly out of view. Use the scroll bar below the network map to display the icons. To separate the icons press **Ctrl** and drag and drop the icon to the new location. Repeat until all the nodes are visible on the graphic area.

Step 3 Verify node accessibility. In the network view, all node icons must be either green, yellow, orange, or red.

If all network nodes do not appear after a few minutes, or if a node icon is gray with an IP address under it, do not continue. Look at the Net box in the lower right corner of the window. If it is gray, log in again, making sure not to check the Disable Network check box on the CTC Login dialog box. If problems persist, see Chapter 4, "Turn Up Network" to review the network turn-up procedure appropriate for your network topology, or refer to the *Cisco ONS 15327 Troubleshooting Guide* for troubleshooting procedures.

Step 4 Verify DCC connectivity. All nodes must be connected by green lines. If lines are missing or gray in color, do not continue. See Chapter 4, "Turn Up Network" and follow the network turn-up procedure appropriate for your network topology. Verify that all nodes have DCC connectivity before continuing.

Step 5 Investigate and resolve, if necessary, all critical (red node icon) or major (orange node icon) alarms. Click the **Alarms** tab to view alarm descriptions. Refer to the *Cisco ONS 15327 Troubleshooting Guide* to resolve alarms before continuing.

Step 6 From the View menu choose **Go to Home View**. Verify that the node is provisioned according to your site or engineering plan:

a. View the cards on the shelf map. Verify that the ONS 15327 cards appear in the specified slots.

b. Click the **Provisioning > General** tabs. Verify that the node name, contacts, date, time, and NTP/SNTP server IP address (if used) are correctly provisioned. If needed, make corrections using the"NTP-B81 Change Node Management Information" procedure on page 10-2.

c. Click the **Network** tab. Verify that the IP address, Subnet mask, Default Router, Prevent LCD IP Config, and Gateway Settings are correctly provisioned. If not, make corrections using the "NTP-B201 Change CTC Network Access" procedure on page 10-4.

d. Click the **Protection** tab. Verify that protection groups are created as specified in your site plan. If the protection groups are not created, complete the "NTP-B170 Create Optical Protection Groups" procedure on page 3-20.

e. If the node is in a BLSR, click the **BLSR** tab. (If the node is not in a BLSR, continue with Step f.) Verify that the following items are provisioned as specified in your site plan:

- BLSR type (2-Fiber)
- BLSR ring ID and node IDs
- Ring reversion time
- East and west card assignments

If you need to make corrections, see the "NTP-B40 Provision BLSR Nodes" procedure on page 4-13 for instructions.

f. Click the **Security** tab. Verify that the users and access levels are provisioned as specified. If not, see the "NTP-B30 Create Users and Assign Security" procedure on page 3-3 to correct the information.

g. If SNMP is used, click the **SNMP** tab and verify the trap and destination information. If the information is correct, see the "NTP-B87 Change SNMP Settings" procedure on page 10-23 to correct the information.

h. Click the **SONET DCC** tab. Verify that SDCC(s) were created to the applicable OC-N slots and ports. If DCCs were not created for the appropriate OC-N slots and ports, see Chapter 4, "Turn Up Network" and complete the turn-up procedure appropriate for your network topology.

i. Click the **Timing** tab. Verify that timing is provisioned as specified. If not, use the "NTP-B85 Change Node Timing" procedure on page 10-15 to make the changes.

j. Click the **Alarm Behavior** tab. If you provisioned optional alarm profiles, verify that the alarms are provisioned as specified. If not, see the "NTP-B70 Create, Download, and Assign Alarm Severity Profiles" procedure on page 6-15 to change the information.

k. Verify that the network element defaults listed in the status area of the node view window is correct.

Step 7 Repeat Step 6 for each node in the network.

Step 8 As appropriate, complete the circuit creation procedure listed on page 5-1.

Stop. You have completed this procedure.

NTP-B181 Create an Automatically Routed DS-1 Circuit

Purpose	This procedure creates an automatically routed DS-1 circuit, meaning CTC chooses the circuit route based on the parameters you specify and on the software version.
Tools/Equipment	None
Prerequisite Procedures	NTP-B127 Verify Network Turn Up, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at a node on the network where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-B314 Assign a Name to a Port" task on page 5-14. If not, continue with Step 3.

Step 3 From the View menu choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box (Figure 5-1 on page 5-7), complete the following fields:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters, (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Type—Choose VT. VT cross-connects will carry the DS-1 circuit across the ONS 15327 network.
- Size—VT1.5 is the default. You cannot change it.
- Bidirectional—Leave checked for this circuit.
- Number of circuits—Type the number of DS-1 circuits you want to create. The default is 1. If you are creating multiple circuits with the same slot and sequential port numbers, you can use Auto-ranged to create the circuits automatically.
- Auto-ranged—This check box is automatically selected if you enter more than 1 in the Number of circuits field. Auto-ranging creates identical (same source and destination) sequential circuits automatically. Uncheck this check box if you do not want CTC to create sequential circuits automatically.
- State—Choose a service state to apply to the circuit:

  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and permits loopbacks on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-B230 Change a Circuit State" task on page 8-7.

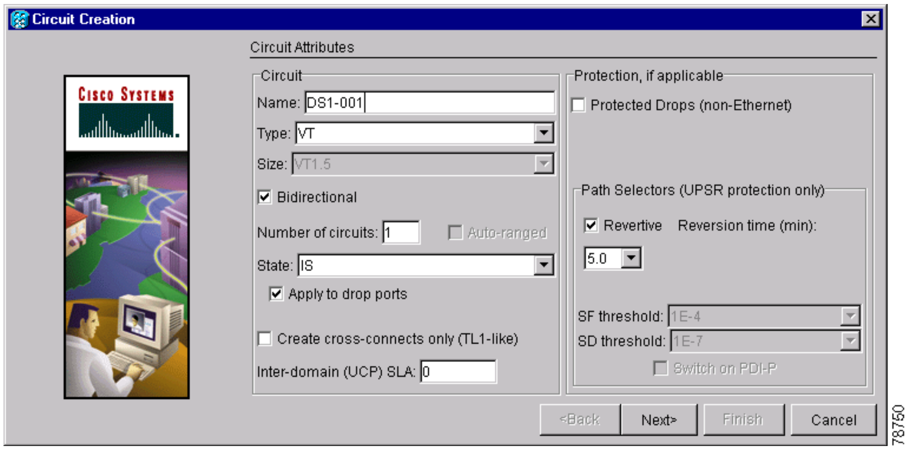
Note If VT circuit source and destination ports are in an OOS_AINS, OOS_MT, or IS state, VT circuits in OOS_AINS will change to IS even if a physical signal is not present. Refer to the *Cisco ONS 15327 Reference Manual* for more information.

- Apply to drop ports—Check this check box you want to apply the state chosen in the State field to the circuit source and destination ports. CTC will apply the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the check box is unchecked, CTC will not change the state of the source and destination ports.

Note LOS alarms are generated if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Check this check box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this box is checked, you cannot assign a name to the circuit. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Inter-domain (UCP) SLA—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Check this check box if you want the circuit routed on protected drops only, that is, to ONS 15327 cards that are in 1:1 or 1+1 protection. If you check this check box, CTC displays only protected cards and ports as source and destination choices.

Figure 5-1 Setting Circuit Attributes For a DS-1 Circuit



Circuit Attributes

Circuit

Name: DS1-001

Type: VT

Size: VT1.5

☑ Bidirectional

Number of circuits: 1 □ Auto-ranged

State: IS

☑ Apply to drop ports

□ Create cross-connects only (TL1-like)

Inter-domain (UCP) SLA: 0

Protection, if applicable

□ Protected Drops (non-Ethernet)

Path Selectors (UPSR protection only)

☑ Revertive Reversion time (min): 5.0

SF threshold: 1E-4

SD threshold: 1E-7

□ Switch on PDI-P

Step 6 If the circuit will be routed on a UPSR, complete the "DLP-B218 Provision UPSR Selectors During Circuit Creation" task on page 5-25. Otherwise, continue with the next step.

Step 7 Click **Next**.

Step 8 Complete the "DLP-B95 Provision a DS-1 Circuit Source and Destination" task on page 5-15.

Step 9 In the Circuit Routing Preferences area (Figure 5-2), click **Route Automatically**. Two options are available; choose either, both, or none based on your preferences.

- Using Required Nodes/Spans—Check this check box if you want to specify nodes and spans to include or exclude in the CTC-generated circuit route.
- Review Route Before Creation—Check this check box if you want to review and edit the circuit route before the circuit is created.

Step 10 Set the circuit path protection:

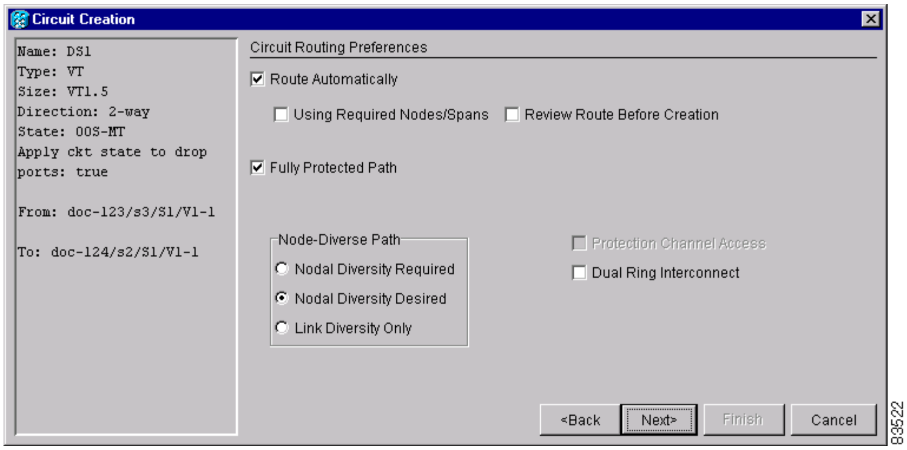
- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 11. CTC creates a fully-protected circuit route based on the path diversity option you choose. Fully-protected paths may or may not have UPSR path segments (with primary and alternate paths), and the path diversity options apply only to UPSR path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with .
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** on the Warning dialog box, and then continue with .

Caution Circuits routed on BLSR protection channels are not protected. They are preempted during BLSR switches.

Step 11 If you selected Fully Protected Path in Step 10, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within UPSR portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the UPSR portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for UPSR portions of the complete circuit path are needed. The paths may be node-diverse, but CTC does not check for node diversity.

Figure 5-2 Setting Circuit Routing Preferences for a DS-1 Circuit



```
Name: DS1
Type: VT
Size: VT1.5
Direction: 2-way
State: OOS-MT
Apply ckt state to drop
ports: true

From: doc-123/s3/S1/V1-1

To: doc-124/s2/S1/V1-1
```

Circuit Routing Preferences

☑ Route Automatically

□ Using Required Nodes/Spans □ Review Route Before Creation

☑ Fully Protected Path

Node-Diverse Path
○ Nodal Diversity Required
● Nodal Diversity Desired
○ Link Diversity Only

□ Protection Channel Access
□ Dual Ring Interconnect

Step 12 If you selected Using Required Nodes/Spans in Step 9, complete the following substeps. If not, continue with Step 13.

a. Click **Next**.

b. In the Circuit Route Constraints area, click a node or span on the circuit map.

c. Click **Include** to include the node or span in the circuit. Click **Exclude** to exclude the node or span from the circuit. The order in which you choose included nodes and spans is the order in which the circuit will be routed. Click spans twice to change the circuit direction.

d. Repeat Step c for each node or span you wish to include or exclude.

e. Review the circuit route. To change the circuit routing order, choose a node from the Required Nodes/Lines or Excluded Notes Links lists and click the **Up** or **Down** buttons to change the circuit routing order. Click **Remove** to remove a node or span.

Step 13 If you selected Review Route Before Creation in Step 9, complete the following substeps. If not, continue with Step 14.

a. Click **Next**.

b. If the DS-1 circuit passes through a node that does not have a VT tunnel, CTC will ask whether you want to create one. See Step 14 for information about the VT tunnel.

c. Review the circuit route. To add or delete a circuit span, choose a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

d. If the provisioned circuit does not reflect the routing and configuration you want, click **Back** to verify and change circuit information. If the circuit needs to be routed to a different path, see the "NTP-B182 Create a Manually Routed DS-1 Circuit" procedure on page 5-9.

Step 14 Click **Finish**. One of the following results occurs, depending on the circuit properties you chose in the Circuit Creation dialog box:

- If the DS-1 circuit passes through a node that does not have a VT tunnel, or if an existing tunnel is full, CTC asks whether you want to create a tunnel. VT tunnels allow VT circuits to pass through ONS 15454s without consuming cross-connect card resources. VT tunnels can carry 28 VT1.5 circuits. In general, creating VT tunnels is a good idea if you are creating many VT circuits from the same source and destination. Refer to the *Cisco ONS 15327 Reference Manual* for more information.

- If you entered more than 1 in the Number of Circuits field and selected Auto-ranged, CTC automatically creates the number of circuits entered in the Number of Circuits field. If auto ranging cannot complete all the circuits, for example, because sequential ports are unavailable at the source or destination, a dialog box appears. Set the new source or destination for the remaining circuits, then click **Finish** to continue auto ranging.
- If you entered more than 1 in the Number of Circuits field and did not choose Auto-ranged, the Circuit Creation dialog box appears for you to create the remaining circuits. Repeat this procedure for each additional circuit.
- After completing the circuit(s), CTC displays the Circuits window.

Step 15 On the Circuits window, verify that the new circuit(s) appear in the circuits list.

Step 16 Complete the "NTP-B135 Test Electrical Circuits" procedure on page 5-33. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-B182 Create a Manually Routed DS-1 Circuit

Purpose	This procedure creates a DS-1 circuit and provision its circuit route.
Tools/Equipment	None
Prerequisite Procedures	NTP-B127 Verify Network Turn Up, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at a node on the network where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-B314 Assign a Name to a Port" task on page 5-14. If not, continue with Step 3. CTC will assign a circuit name automatically based on circuit type, node name, and sequence number.

Step 3 From the View menu choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box (see Figure 5-1 on page 5-7), complete the following fields:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Type—Choose VT. VT cross-connects will carry the DS-1 circuit across the ONS 15327 network.
- Size—VT1.5 is the default. You cannot change it.
- Bidirectional—Leave checked for this circuit.
- Number of circuits—Type the number of DS-1 circuits you want to create. The default is 1.
- Auto-ranged—Applies to automatically-routed circuits only. If you entered more than 1 in Number of Circuits, uncheck this check box. (The check box is unavailable if only one circuit is entered in Number of Circuits.)

- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and permits loopbacks on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-B230 Change a Circuit State" task on page 8-7.

Note If VT circuit source and destination ports are in an OOS_AINS, OOS_MT, or IS state, VT circuits in OOS_AINS will change to IS even if a physical signal is not present. Refer to the *Cisco ONS 15327 Reference Manual* for more information.

- Apply to drop ports—Check this check box if you want to apply the state chosen in the State field to the circuit source and destination ports. CTC will apply the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the check box is unchecked, CTC will not change the state of the source and destination ports.

Note LOS alarms appear if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Check this check box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this box is checked, you cannot assign a name to the circuit. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Inter-domain (UCP) SLA—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Check this check box if you want the circuit routed on protected drops only, that is, to ONS 15327 cards that are in 1:1 or 1+1 protection. If you check this check box, CTC displays only protected cards and ports as source and destination choices.

Step 6 If the circuit will be routed on a UPSR, complete the "DLP-B218 Provision UPSR Selectors During Circuit Creation" task on page 5-25. Otherwise, continue with the next step.

Step 7 Click **Next**.

Step 8 Complete the "DLP-B95 Provision a DS-1 Circuit Source and Destination" task on page 5-15.

Step 9 In the Circuit Routing Preferences area (see Figure 5-2 on page 5-8), uncheck **Route Automatically**.

Step 10 Set the circuit path protection:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 11. Fully-protected paths may or may not have UPSR path segments (with primary and alternate paths), and the path diversity options apply only to UPSR path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 12.

- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path,** check **Protection Channel Access**, click **Yes** on the Warning dialog box, and then continue with Step 12.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 11 If you selected Fully Protected Path, choose a Node-Diverse Path option:

- Nodal Diversity Required—Ensures that the primary and alternate paths within the UPSR portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the UPSR portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for UPSR portions of the complete circuit path are needed. The paths may be node-diverse, but CTC does not check for node diversity.

Step 12 When all the circuits are created, the main Circuits window appears. Verify that the circuit(s) you created are correct.

Step 13 Complete the "NTP-B135 Test Electrical Circuits" procedure on page 5-33. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-B183 Create a Unidirectional DS-1 Circuit with Multiple Drops

Purpose	This procedure creates a unidirectional DS-1 circuit with multiple drops (destinations).
Tools/Equipment	None
Prerequisite Procedures	NTP-B127 Verify Network Turn Up, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23at a node on the network where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-B314 Assign a Name to a Port" task on page 5-14. If not, continue with Step 3.

Step 3 From the View menu choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box (Figure 5-3), complete the following fields:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Type—Choose VT.
- Size—VT1.5 is the default. You cannot change it.
- Bidirectional—Uncheck for this circuit.
- Number of circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable when the Number of Circuits field is 1.
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and permits loopbacks on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-B230 Change a Circuit State" task on page 8-7.

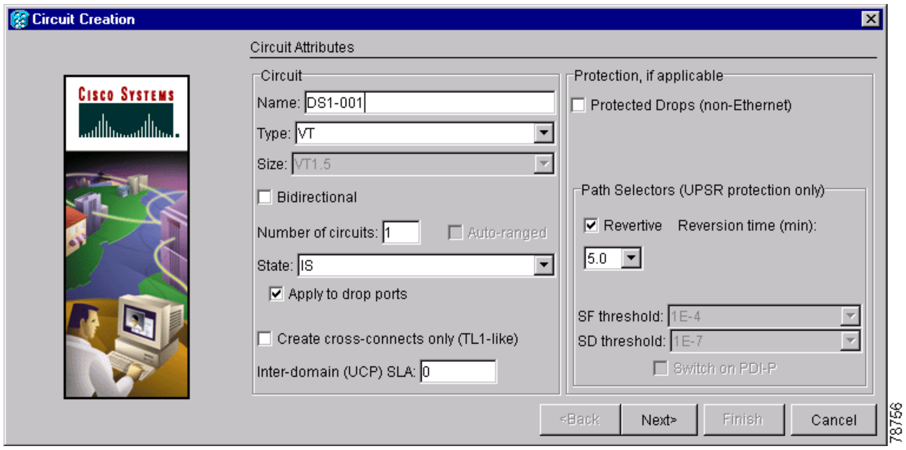
Note If VT circuit source and destination ports are in an OOS_AINS, OOS_MT, or IS state, VT circuits in OOS_AINS will change to IS even if a physical signal is not present. Refer to the *Cisco ONS 15327 Reference Manual* for more information.

- Apply to drop ports—Check this check box if you want to apply the state chosen in the State field to the circuit source and destination ports. CTC will apply the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the check box is unchecked, CTC will not change the state of the source and destination ports.

Note LOS alarms appear if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Check this check box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this check box is checked, you cannot assign a name to the circuit. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Inter-domain (UCP) SLA—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Check this check box if you want the circuit routed to protect drops only, that is, to ONS 15327 cards that are in 1:1 or 1+1 protection. If you check this check box, CTC displays only protected ports as source and destination choices.

Figure 5-3 Setting Circuit Attributes for a Unidirectional DS-1 Circuit



Circuit Creation

Circuit Attributes

Circuit

Name: DS1-001

Type: VT

Size: VT1.5

□ Bidirectional

Number of circuits: 1 □ Auto-ranged

State: IS

☑ Apply to drop ports

□ Create cross-connects only (TL1-like)

Inter-domain (UCP) SLA: 0

Protection, if applicable

□ Protected Drops (non-Ethernet)

Path Selectors (UPSR protection only)

☑ Revertive Reversion time (min): 5.0

SF threshold: 1E-4

SD threshold: 1E-7

□ Switch on PDI-P

Step 6 Click **Next**.

Step 7 Complete the "DLP-B95 Provision a DS-1 Circuit Source and Destination" task on page 5-15.

Step 8 In the Circuit Routing Preferences area, uncheck **Route Automatically**. When Route Automatically is not selected, Using Required Nodes/Spans and Review Route Before Circuit Creation are unavailable.

Step 9 Set the circuit path protection:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 11. Fully-protected paths may or may not have UPSR path segments (with primary and alternate paths), and the path diversity options apply only to UPSR path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 11.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** on the Warning dialog box, and then continue with Step 11.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 10 If you selected Fully Protected Path, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within the UPSR portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the UPSR portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for UPSR portions of the complete circuit path are needed. The paths may be node-diverse, but CTC does not check for node diversity.

Step 11 On the Circuits window, click the circuit that you want to route to multiple drops. The Delete, Edit, and Search buttons become active.

Step 12 Click **Edit** (or double-click the circuit row). The Edit Circuit window appears with the General tab selected.

All nodes in the DCC network appear on the network map. Circuit source and destination information appears under the source and destination nodes. To display a detailed view of the circuit, click **Show Detailed Map**. To rearrange a node icon, select the node, press **Ctrl**, then drag and drop the icon to the new location.

Step 13 On the Edit Circuit dialog box, click the **Drops** tab. A list of existing drops appears.

Step 14 Click **Create**.

Step 15 On the Define New Drop dialog box, create the new drop:

a. Node—Choose the target node for the circuit drop.

b. Slot—Choose the target card and slot.

c. Port, STS, VT, or DS1—Choose the port, STS, VT, or DS1 from the Port, STS, VT or DS1 drop-down menus. The card selected in Step b determines the fields that appear. See Table 5-2 on page 5-2 for a list of options.

d. The routing preferences for the new drop will match those of the original circuit. However, you can modify the following:

   - If the original circuit was routed on a protected path, you can change the nodal diversity options: [Required, Desired, Don't Care; Link Diverse only]. See Step 10 for options descriptions.
   - If the original circuit was not routed on a protected path, the Protection Channel Access options is available. See Step 9 for a description of the PCA option.

e. Click **OK**. The new drop appears in the Drops list.

Step 16 If you need to create additional drops for the circuit, repeat Steps 14 and 15 to create the additional drops.

Step 17 Choose **Close**. The Circuits window appears.

Step 18 Verify that the new drops appear in the Destination column for the circuit you edited. If they do not appear repeat Steps 5 through 22, making sure all options are provisioned correctly.

Step 19 Complete the "NTP-B135 Test Electrical Circuits" procedure on page 5-33. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

DLP-B314 Assign a Name to a Port

Purpose	This task assigns a name to an ONS 15327 port.
Tools/Equipment	None
Prerequisite Procedures	NTP-B24 Verify Card Installation, page 3-2
Required/As Needed	As needed.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Double-click the OC-N or XTC card that has the port you want to provision.

Step 2 Click the **Provisioning** tab.

Step 3 Click the **Port Name** column for the port number you are assigning a name to and enter the desired port name.

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

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-B95 Provision a DS-1 Circuit Source and Destination

Purpose	This task provisions an electrical circuit source and destination for a DS-1 circuit.
Tools/Equipment	None
Prerequisite Procedures	You perform this task during one of the following procedures: NTP-B181 Create an Automatically Routed DS-1 Circuit, page 5-5, or NTP-B182 Create a Manually Routed DS-1 Circuit, page 5-9, or NTP-B183 Create a Unidirectional DS-1 Circuit with Multiple Drops, page 5-11
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note After you have selected the circuit properties in the Circuit Source dialog box according to the specific circuit creation procedure, you are ready to provision the circuit source.

Step 1 From the Node drop-down menu choose the node where the source will originate.

Step 2 From the Slot drop-down menu choose the slot containing the XTC card where the circuit will originate.

Step 3 From the DS-1 drop-down menu choose the source DS-1.

Step 4 If you need to create a secondary source, for example, a UPSR bridge/selector circuit entry point in a multivendor UPSR, click **Use Secondary Source** and repeat Steps 1 through 3 to define the secondary source. If you do not need to create a secondary source, continue with Step 5.

Step 5 Click **Next**.

Step 6 From the Node drop-down menu choose the destination (termination) node.

Step 7 From the Slot drop-down menu choose the slot containing the destination card. The destination is typically an XTC card. You can also choose an OC-N card to map the DS-1 to a VT1.5 for optical transport.

Step 8 Depending on the destination card, choose the destination port, STS, VT, or DS1 from the sub-menus that appear based on the card selected in Step 7. See Table 5-2 on page 5-2 for a list of valid options. CTC does not display ports, STSs, VTs, or DS1s already used by other circuits. If you and a user working on the same network choose the same port, STS, VT, port, or DS1 simultaneously, one of you will receive a Path in Use error and be unable to complete the circuit. The user with the incomplete circuit needs to choose new destination parameters.

Step 9 If you need to create a secondary destination, for example, a UPSR bridge/selector circuit exit point in a multivendor UPSR, click **Use Secondary Destination** and repeat Steps 6–8 to define the secondary destination.

Step 10 Click **Next**.

Step 11 Return to your originating procedure (NTP).

NTP-B184 Create an Automatically Routed DS-3 Circuit

Purpose	This procedure creates an automatically routed DS-3 circuit. CTC routes the circuit automatically based on circuit creation parameters and the software version.
Tools/Equipment	None
Prerequisite Procedures	NTP-B127 Verify Network Turn Up, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at a node on the network where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-B314 Assign a Name to a Port" task on page 5-14. If not, continue with Step 3.

Step 3 From the View menu choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box (Figure 5-4), complete the following fields:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Type—Choose STS. STS cross-connects will carry the DS-3 circuit across the ONS 15327 network.
- Size—Choose STS-1.
- Bidirectional—Leave checked for this circuit.
- Number of circuits—Type the number of DS-3 circuits you want to create. The default is 1. If you are creating multiple circuits with sequential source and destination ports, you can use Auto-ranged to create the circuits automatically.
- Auto-ranged—This check box is automatically selected if you enter more than 1 in the Number of circuits field. Leave selected if you are creating multiple DS-3 circuits with the same source and destination and you want CTC to create the circuits automatically. Uncheck this check box if you do not want CTC to create sequential circuits automatically.
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).

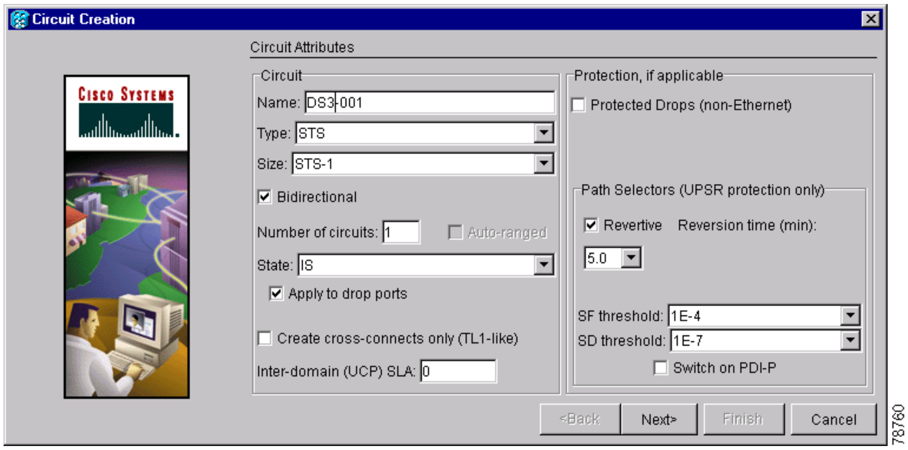
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and permits loopbacks on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-B230 Change a Circuit State" task on page 8-7.

- Apply to drop ports—Check this check box if you want to apply the state chosen in the State field to the circuit source and destination ports. CTC will apply the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the check box is unchecked, CTC will not change the state of the source and destination ports.

Note LOS alarms appear if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Check this check box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this box is checked, you cannot assign a name to the circuit. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Inter-domain (UCP) SLA—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Check this check box if you want the circuit routed on protected drops only, that is, to ONS 15327 cards that are in 1:1 or 1+1 protection. If you check this check box, CTC displays only protected cards and ports as source and destination choices.

Figure 5-4 Setting Circuit Attributes for a DS-3



Circuit Creation

Circuit Attributes

Circuit

Name: DS3-001

Type: STS

Size: STS-1

☑ Bidirectional

Number of circuits: 1 □ Auto-ranged

State: IS

☑ Apply to drop ports

□ Create cross-connects only (TL1-like)

Inter-domain (UCP) SLA: 0

Protection, if applicable

□ Protected Drops (non-Ethernet)

Path Selectors (UPSR protection only)

☑ Revertive Reversion time (min): 5.0

SF threshold: 1E-4

SD threshold: 1E-7

□ Switch on PDI-P

Step 6 If the circuit will be routed on a UPSR, complete the "DLP-B218 Provision UPSR Selectors During Circuit Creation" task on page 5-25.

Step 7 Click **Next**.

Step 8 Complete the "DLP-B208 Provision a DS-3 Circuit Source and Destination" task on page 5-26.

Step 9 In the Circuit Routing Preferences area (Figure 5-5 on page 5-18), choose **Route Automatically**. Two options are available; choose either, both, or none based on your preferences.:

- Using Required Nodes/Spans—Check this check box to specify nodes and spans to include or exclude in the CTC-generated circuit route.
- Review Route Before Creation—Check this check box to review and edit the circuit route before the circuit is created.

Step 10 Set the circuit path protection:

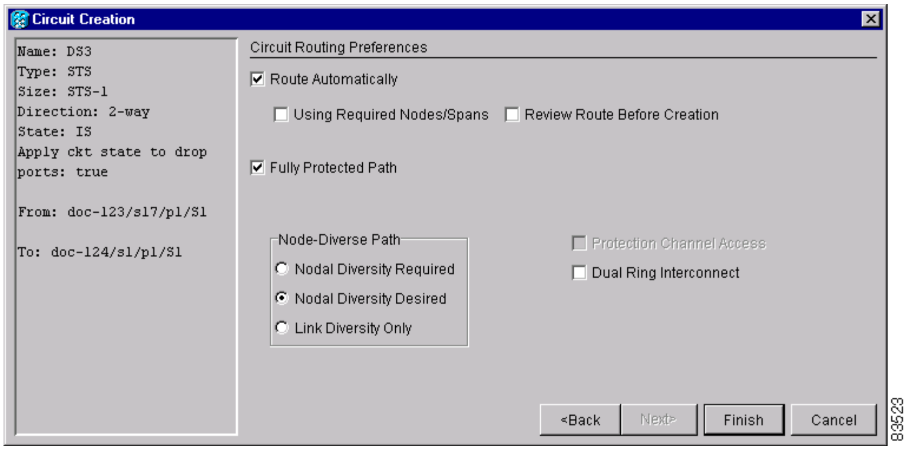
- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 11. CTC creates a fully-protected circuit route based on the path diversity option you choose. Fully-protected paths may or may not have UPSR path segments (with primary and alternate paths), and the path diversity options apply only to UPSR path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 12.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** on the Warning dialog box, and then continue with Step 12.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 11 If you selected Fully Protected Path in Step 10, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within UPSR portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the UPSR portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for UPSR portions of the complete circuit path are needed. The paths may be node-diverse, but CTC does not check for node diversity.

Figure 5-5 Setting Circuit Routing Preferences for a DS-3 Circuit



Circuit Creation

```
Name: DS3
Type: STS
Size: STS-1
Direction: 2-way
State: IS
Apply ckt state to drop
ports: true

From: doc-123/s17/p1/S1

To: doc-124/s1/p1/S1
```

Circuit Routing Preferences

☑ Route Automatically

□ Using Required Nodes/Spans □ Review Route Before Creation

☑ Fully Protected Path

Node-Diverse Path
○ Nodal Diversity Required
● Nodal Diversity Desired
○ Link Diversity Only

□ Protection Channel Access
□ Dual Ring Interconnect

Step 12 If you selected Using Required Nodes/Spans in Step 9, complete the following substeps; otherwise, continue with Step 13:

a. Click **Next**.

b. In the Circuit Route Constraints area, click a node or span on the circuit map.

c. Click **Include** to include the node or span in the circuit. Click **Exclude** to exclude the node or span from the circuit. The order in which you choose included nodes and spans determines the circuit sequence. Click spans twice to change the circuit direction.

d. Repeat Step c for each node or span you wish to include or exclude.

e. Review the circuit route. To change the circuit routing order, choose a node from the Required Nodes/Lines or Excluded Notes Links lists, then click the **Up** or **Down** buttons to change the circuit routing order. Click **Remove** to remove a node or span.

Note If a node or span stays gray, that node or span is required.

Step 13 If you selected Review Route Before Creation, complete the following substeps; otherwise, continue with Step 14.

a. Click **Next**.

b. Review the circuit route. To add or delete a circuit span, choose a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

c. If the provisioned circuit does not reflect the routing and configuration you want, click **Back** to verify and change circuit information. If the circuit needs to be routed to a different path, see the "NTP-B185 Create a Manually Routed DS-3 Circuit" procedure on page 5-20.

Step 14 Click **Finish**. One of the following actions occurs based on the circuit properties you selected:

- If you entered more than 1 in the Number of Circuits field and selected Auto-ranged, CTC automatically creates the number of circuits entered in the Number of Circuits field. If auto ranging cannot complete all the circuits, for example, because sequential ports are unavailable at the source or destination, a dialog box appears. Set the new source or destination for the remaining circuits, then click **Finish** to continue auto ranging.
- If you entered more than 1 in the Number of Circuits field and did not choose Auto-ranged, the Circuit Creation dialog box appears for you to create the remaining circuits. Repeat Steps 8–14 for each additional circuit.
- After completing the circuit(s), CTC displays the Circuits window.

Step 15 On the Circuits window, verify that the circuit(s) you just created appear in the circuits list.

Step 16 Complete the "NTP-B135 Test Electrical Circuits" procedure on page 5-33. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-B185 Create a Manually Routed DS-3 Circuit

Purpose	This procedure creates a DS-3 circuit and allows you to choose the circuit route.
Tools/Equipment	None
Prerequisite Procedures	NTP-B127 Verify Network Turn Up, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at a node on the network where you will create the circuit. If you are already logged in, continue with Step 3.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-B314 Assign a Name to a Port" task on page 5-14. If not, continue with Step 4.

Step 3 From the View menu choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box (Figure 5-4 on page 5-17), complete the following fields:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave this field blank, CTC will assign a default name to the circuit.
- Type—Choose STS. STS cross-connects will carry the DS-3 circuit across the ONS 15327 network.
- Size—Choose STS-1.
- Bidirectional—Leave this field checked.
- Number of circuits—Type the number of DS-3 circuits you want to create. The default is 1.
- Auto-ranged—Applies to automatically-routed circuits only. If you entered more than 1 in Number of Circuits, uncheck this check box. (The check box is unavailable if only one circuit is entered in Number of Circuits.)
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and permits loopbacks on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-B230 Change a Circuit State" task on page 8-7.
- Apply to drop ports—Check this check box if you want to apply the state chosen in the *State* field to the circuit source and destination ports. CTC will apply the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the check box is unchecked, CTC will not change the state of the source and destination ports.

Note LOS alarms appear if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Check this check box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this box is checked, you cannot assign a name to the circuit. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Inter-domain (UCP) SLA—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Check this check box if you want the circuit routed to protect drops only, that is, to ONS 15327 cards that are in 1:1 or 1+1 protection. If you check this check box, CTC displays only protected cards as source and destination choices.

Step 6 If the circuit will be routed on a UPSR, complete the "DLP-B218 Provision UPSR Selectors During Circuit Creation" task on page 5-25.

Step 7 Click **Next**.

Step 8 Complete the "DLP-B208 Provision a DS-3 Circuit Source and Destination" task on page 5-26.

Step 9 In the Circuit Routing Preferences area (Figure 5-5 on page 5-18), uncheck **Route Automatically**.

Step 10 Set the circuit path protection:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 11. Fully-protected paths may or may not have UPSR path segments (with primary and alternate paths), and the path diversity options apply only to UPSR path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 12.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** on the Warning dialog box, and then continue with Step 12.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 11 If you selected Fully Protected Path, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within the UPSR portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the UPSR portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for UPSR portions of the complete circuit path are needed. The paths may be node-diverse, but CTC does not check for node diversity.

Step 12 Click **Next**. In the Route Review and Edit area, node icons appear for you to route the circuit manually. The green arrows pointing from the selected node to other network nodes indicate spans that are available for routing the circuit.

Step 13 Complete the "DLP-B96 Provision a DS-1 or DS-3 Circuit Route" task on page 5-27 for the DS-3 circuit you are creating.

Step 14 Click **Finish**. If you entered more than 1 in the Number of Circuits field, the Circuit Creation dialog box appears for you to create the remaining circuits. Repeat this procedure for each additional circuit.

Step 15 When all the circuits are created, CTC displays the main Circuits window. Verify that the circuit(s) you created appear in the window.

Step 16 Complete the "NTP-B135 Test Electrical Circuits" procedure on page 5-33. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-B186 Create a Unidirectional DS-3 Circuit with Multiple Drops

Purpose	This procedure creates a unidirectional DS-3 circuit with multiple drops.
Tools/Equipment	None
Prerequisite Procedures	NTP-B127 Verify Network Turn Up, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at a node on the network where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-B314 Assign a Name to a Port" task on page 5-14. If not, continue with Step 3.

Step 3 From the View menu choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box (Figure 5-6 on page 5-23), complete the following fields:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Type—Choose STS.
- Size—Choose STS-1.
- Bidirectional—Uncheck for this circuit.
- Number of circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable when the Number of Circuits is 1.
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).

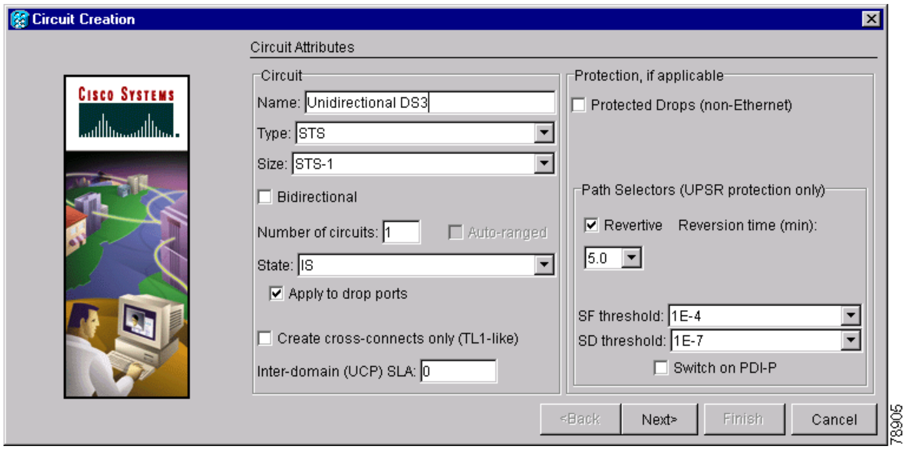
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and permits loopbacks on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-B230 Change a Circuit State" task on page 8-7.

- Apply to drop ports—Check this check box if you want to apply the state chosen in the *State* field to the circuit source and destination ports. CTC will apply the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the check box is unchecked, CTC will not change the state of the source and destination ports.

Note LOS alarms appear if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Check this check box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this box is checked, you cannot assign a name to the circuit. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Inter-domain (UCP) SLA—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Check this check box if you want the circuit routed to protect drops only, that is, to ONS 15327 cards that are in 1:1 or 1+1 protection. If you check this check box, CTC displays only protected cards as source and destination choices.

Figure 5-6 Setting Circuit Attributes for a Unidirectional DS-3 Circuit



Circuit Attributes

Circuit

Name: Unidirectional DS3

Type: STS

Size: STS-1

□ Bidirectional

Number of circuits: 1 □ Auto-ranged

State: IS

☑ Apply to drop ports

□ Create cross-connects only (TL1-like)

Inter-domain (UCP) SLA: 0

Protection, if applicable

□ Protected Drops (non-Ethernet)

Path Selectors (UPSR protection only)

☑ Revertive Reversion time (min): 5.0

SF threshold: 1E-4

SD threshold: 1E-7

□ Switch on PDI-P

Step 6 If the circuit will be routed on a UPSR, set the UPSR path selectors. See the "DLP-B218 Provision UPSR Selectors During Circuit Creation" task on page 5-25.

Step 7 Click **Next**.

Step 8 Complete the "DLP-B208 Provision a DS-3 Circuit Source and Destination" task on page 5-26.

Step 9 Uncheck **Route Automatically**. When Route Automatically is not selected, Using Required Nodes/Spans and Review Route Before Circuit Creation are unavailable.

Step 10 Set the circuit path protection:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 11. Fully-protected paths may or may not have UPSR path segments (with primary and alternate paths), and the path diversity options apply only to UPSR path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 13.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** on the Warning dialog box, and then continue with Step 13.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 11 If you selected Fully Protected Path, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within the UPSR portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the UPSR portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for UPSR portions of the complete circuit path are needed. The paths may be node-diverse, but CTC does not check for node diversity.

Step 12 If you selected Fully Protected Path and the circuit will be routed on a UPSR dual ring interconnect (DRI), check the **Dual Ring Interconnect** check box.

Step 13 Click **Next**. In the Route Review and Edit area, node icons appear for you to route the circuit manually. The circuit source node is selected. Green arrows pointing from the source node to other network nodes indicate spans that are available for routing the circuit.

Step 14 Complete the "DLP-B96 Provision a DS-1 or DS-3 Circuit Route" task on page 5-27 for the DS-3 you are creating.

Step 15 Click **Finish**. After completing the circuit, CTC displays the Circuits window.

Step 16 On the Circuits window, click the circuit that you want to route to multiple drops. The Delete, Edit, and Search radio buttons become active.

Step 17 Click **Edit**. The Edit Circuit window appears with the General tab selected. All nodes in the DCC network appear on the network map. Circuit source and destination information appears under the source and destination nodes. To display a detailed view of the circuit, click **Show Detailed Map**. You can rearrange the node icons by selecting the node with the left mouse button while simultaneously pressing **Ctrl**, then dragging the icon to the new location.

Step 18 On the Edit Circuit dialog box, click the **Drops** tab. A list of existing drops appears.

Step 19 Click **Create**.

Step 20 On the Define New Drop dialog box, define the new drop:

a. Node—Choose the target node for the circuit drop.

b. Slot—Choose the target card and slot

c. Port, STS—Choose the port and/or STS from the Port and STS drop-down menus. The card selected in Step b determines whether port, STS, or both display. See Table 5-2 on page 5-2 for a list of options.

d. The routing preferences for the new drop will match those of the original circuit. However, you can modify the following:

- If the original circuit was routed on a protected path, you can change the nodal diversity options: [Required, Desired, Don't Care; Link Diverse only]. See Step 11 for options descriptions.
- If the original circuit was not routed on a protected path, the Protection Channel Access options is available. See Step 10 for a description of the PCA option.

e. Click **OK**. The new drop appears in the Drops list.

Step 21 If you need to create additional drops for the circuit, repeat Steps 19 and 20 to create the additional drops.

Step 22 Click **Close**. The Circuits window displays.

Step 23 Verify that the new drops appear in the Destination column for the circuit you edited. If they do not appear, repeat this procedure, making sure all options are provisioned correctly.

Step 24 Complete the "NTP-B135 Test Electrical Circuits" procedure on page 5-33. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

DLP-B218 Provision UPSR Selectors During Circuit Creation

Purpose	This task provisions UPSR selectors during circuit creation. Complete this task only if the circuit will be routed on a UPSR.
Tools/Equipment	None
Prerequisite Procedures	You must have the Circuit Creation wizard displayed.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 On the Circuit Attributes panel of the Circuit Creation wizard, set the UPSR path selectors:

- Revertive—Check this check box if you want traffic to revert to the working path when the conditions that diverted it to the protect path are repaired. If you do not choose Revertive, traffic remains on the protect path after the switch.
- Reversion time—If Revertive is checked, click the Reversion time field and choose a reversion time from the drop-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working path. Traffic can revert when conditions causing the switch are cleared.
- SF threshold—For STS circuits, set the UPSR path-level signal failure bit error rate (BER) thresholds. Unavailable for VT circuits.
- SD threshold—For STS circuits, set the UPSR path-level signal degrade BER thresholds. Unavailable for VT circuits.
- Switch on PDI-P—For STS circuits, check this check box if you want traffic to switch when an STS payload defect indicator is received. Unavailable for VT circuits.

Step 2 Return to your originating procedure (NTP).

DLP-B208 Provision a DS-3 Circuit Source and Destination

Purpose	This task provisions an electrical circuit source and destination for a DS-3 circuit.
Tools/Equipment	None
Prerequisite Procedures	You perform this task during one of the following procedures: NTP-B184 Create an Automatically Routed DS-3 Circuit, page 5-16, or NTP-B185 Create a Manually Routed DS-3 Circuit, page 5-20, or NTP-B186 Create a Unidirectional DS-3 Circuit with Multiple Drops, page 5-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note After you have selected the circuit properties in the Circuit Source dialog box according to the specific circuit creation procedure, you are ready to provision the circuit source.

Step 1 From the Node drop-down menu choose the node where the source will originate.

Step 2 From the Slot drop-down menu choose the slot containing the XTC card where the circuit will originate

Step 3 From the Port drop-down menu choose the source XTC card as appropriate.

Step 4 If you need to create a secondary source, for example, a UPSR bridge/selector circuit entry point in a multivendor UPSR, click **Use Secondary Source** and repeat Steps 1 through 3 to define the secondary source. If you do not need to create a secondary source, continue with Step 5.

Step 5 Click **Next**.

Step 6 From the Node drop-down menu choose the destination (termination) node.

Step 7 From the Slot drop-down menu choose the slot containing the destination card. The destination is typically a XTC card. You can also choose an OC-N card to the map DS-3 circuit to an STS.

Step 8 Depending on the destination card, choose the destination port or STS from the sub-menus that display based on the card selected in Step 3. See Table 5-2 on page 5-2 for a list of valid options. CTC does not display ports, STSs, VTs, or DS1s if they are already in use by other circuits. If you and a user working on the same network choose the same port, STS, VT, port, or DS1 simultaneously, one of you will receive a Path in Use error and be unable to complete the circuit. The user with the incomplete circuit needs to choose new destination parameters.

Step 9 If you need to create a secondary destination, for example, a UPSR bridge/selector circuit exit point in a multivendor UPSR, click **Use Secondary Destination** and repeat Steps 6 and 7 to define the secondary destination.

Step 10 Click **Next**.

Step 11 Return to your originating procedure (NTP).

DLP-B96 Provision a DS-1 or DS-3 Circuit Route

Purpose	This task provisions the circuit route for manually-routed DS-1 or DS-3 circuits.
Tools/Equipment	None
Prerequisite Procedures	You perform this task during one of the following procedures: NTP-B182 Create a Manually Routed DS-1 Circuit, page 5-9, or NTP-B183 Create a Unidirectional DS-1 Circuit with Multiple Drops, page 5-11, or NTP-B185 Create a Manually Routed DS-3 Circuit, page 5-20, or NTP-B186 Create a Unidirectional DS-3 Circuit with Multiple Drops, page 5-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 On the Circuit Creation wizard in the Route Review and Edit area, click the source node icon if it is not already selected.

Step 2 Starting with a span on the source node, click the arrow of the span you want the circuit to travel. The arrow turns white. In the Selected Span area, the From and To fields display span information. The source STS and VT (DS-1 circuit only) appear.

Step 3 If you want to change the source STS, adjust the Source STS field; otherwise, continue with Step 4.

Step 4 If you want to change the source VT for DS-1 circuits, adjust the Source *VT* field; otherwise, continue with Step 5.

Note VT is gray (unavailable) for DS-3 circuits.

Step 5 Click **Add Span**.The span is added to the Included Spans list and the span arrow turns blue.

Step 6 Repeat Steps 2 through 5 until the circuit is provisioned from the source to the destination node through all intermediary nodes. If the Fully Protect Path field is checked on the Circuit Routing Preferences panel, you must:

- Add two spans for all UPSR or unprotected portions of the circuit route from the source to the destination
- Add one span for all BLSR or 1+1 portions of route from the source to the destination

Step 7 Return to your originating procedure (NTP).

NTP-B133 Create an Automatically Routed VT Tunnel

Purpose	This procedure creates an automatically routed VT tunnel from source to destination nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-B127 Verify Network Turn Up, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note VT tunnels allow VT circuits to pass through intermediary ONS 15327s without consuming VT matrix resources on the cross-connect card. VT tunnels can carry 28 VT1.5 circuits. In general, creating VT tunnels is a good idea if you are creating many VT circuits from the same source and destination. Refer to the Circuits and Tunnels chapter in the *Cisco ONS 15327 Reference Manual* for more information.

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at a node on the network where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the tunnel source and destination ports before you create the circuit, complete the "DLP-B314 Assign a Name to a Port" task on page 5-14. If not, continue with Step 3.

Step 3 From the View menu choose **Go to Network View**.

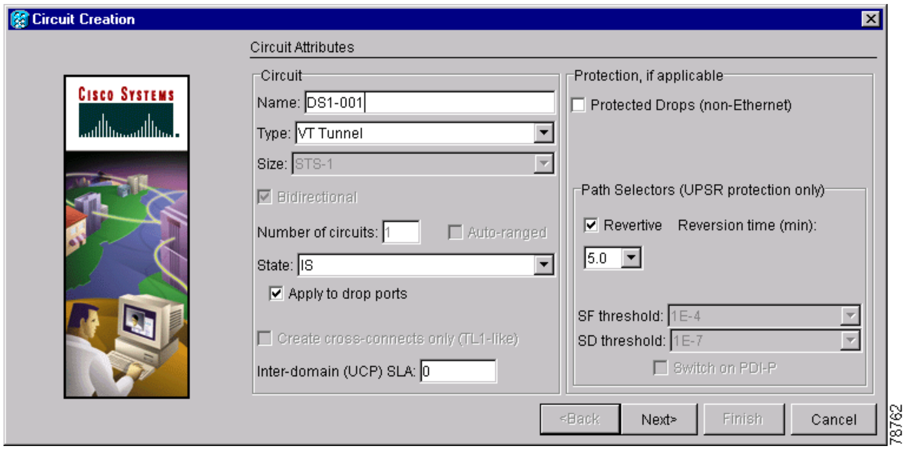
Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box (Figure 5-7), complete the following fields:

- Name—Assign a name to the VT tunnel. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the tunnel.
- Type—Choose VT Tunnel. The Bidirectional, Number of Circuits, Field Size, and Create cross-connects fields in the dialog box become unavailable.
- Size—Unavailable for VT tunnels.
- Bidirectional—Unavailable for VT tunnels.
- Number of circuits—Unavailable for VT tunnels.
- Auto-ranged—Unavailable for VT tunnels.
- State—Choose a service state to apply to the VT tunnel:
  - IS—The VT tunnel is in service.
  - OOS—The VT tunnel is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The VT tunnel is in service when it receives a valid signal; until then, the tunnel is out of service.
  - OOS-MT—The VT tunnel is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and permits loopbacks on the tunnel. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-B230 Change a Circuit State" task on page 8-7.
- Apply to drop ports—Uncheck this check box.

- Inter-domain (UCP) SLA—If the tunnel will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.

Figure 5-7 Setting Attributes for a VT Tunnel



Circuit Attributes

Circuit

Name: DS1-001

Type: VT Tunnel

Size: STS-1

☑ Bidirectional

Number of circuits: 1 □ Auto-ranged

State: IS

☑ Apply to drop ports

□ Create cross-connects only (TL1-like)

Inter-domain (UCP) SLA: 0

Protection, if applicable

□ Protected Drops (non-Ethernet)

Path Selectors (UPSR protection only)

☑ Revertive Reversion time (min): 5.0

SF threshold: 1E-4

SD threshold: 1E-7

□ Switch on PDI-P

Step 6 Click **Next**.

Step 7 In the Circuit Source area, choose the node where the VT tunnel will originate from the Node drop-down menu.

Step 8 Click **Next**.

Step 9 In the Circuit Destination area, choose the node where the VT tunnel will terminate from the Node drop-down menu.

Step 10 Click **Next**.

Step 11 In the Circuit Routing Preferences area, choose **Route Automatically**. Two options are available; choose either, both, or none based on your preferences.

- Using Required Nodes/Spans—Check this check box to specify nodes and spans to include or exclude in the CTC-generated tunnel route.
- Review Route Before Creation—Check this check box to review and edit the VT tunnel route before the circuit is created.

Step 12 If you selected Using Required Nodes/Spans:

a. Click **Next**.

b. In the Circuit Route Constraints area, click a span on the VT tunnel map.

c. Click **Include** to include the node or span in the VT tunnel. Click **Exclude** to exclude the node or span from the VT tunnel. The order in which you choose included nodes and spans sets the VT tunnel sequence. Click spans twice to change the circuit direction.

d. Repeat Step c for each node or span you wish to include or exclude.

e. Review the VT tunnel route. To change the tunnel routing order, choose a node in the Required Nodes/Lines or Excluded Notes Links lists, then click the **Up** or **Down** buttons to change the tunnel routing order. Click **Remove** to remove a node or span.

Step 13 If you selected Review Route Before Creation:

a. Click **Next**.

- **b.** Review the tunnel route. To add or delete a tunnel span, choose a node on the tunnel route. Blue arrows show the tunnel route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.
- **c.** If the provisioned tunnel does not reflect the routing and configuration you want, click **Back** to verify and change tunnel information.

Step 14 Click **Finish**. The Circuits window displays.

Step 15 Verify that the tunnel you just created appears in the circuits list. VT tunnels are identified by VTT in the Type column.

Stop. You have completed this procedure.

NTP-B134 Create a Manually Routed VT Tunnel

Purpose	This procedure creates a manually routed VT tunnel from source to destination nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-B127 Verify Network Turn Up, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note VT tunnels allow VT circuits to pass through intermediary ONS 15327s without consuming VT matrix resources on the cross-connect card. VT tunnels can carry 28 VT1.5 circuits. In general, creating VT tunnels is a good idea if you are creating many VT circuits from the same source and destination. Refer to the Circuits and Tunnels chapter in the *Cisco ONS 15327 Reference Manual* for more information.

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at a node on the network where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the tunnel source and destination ports before you create the circuit, complete the "DLP-B314 Assign a Name to a Port" task on page 5-14. If not, continue with Step 3.

Step 3 From the View menu choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box (Figure 5-1 on page 5-7), complete the following fields:

- Name—Assign a name to the VT tunnel. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the tunnel.
- Type—Choose VT Tunnel. The Bidirectional, Number of Circuits, Field Size, and Create cross-connects fields in the dialog box become unavailable (grayed out).
- Size—Unavailable for VT tunnels.
- Bidirectional—Unavailable for VT tunnels.
- Number of circuits—Unavailable for VT tunnels.

- Auto-ranged—Unavailable for VT tunnels.
- State—Choose a service state to apply to the VT tunnel:
  - IS—The VT tunnel is in service.
  - OOS—The VT tunnel is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The VT tunnel is in service when it receives a valid signal; until then, the circuit is out of service.
  - OOS-MT—The VT tunnel is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and permits loopbacks. Use OOS-MT for testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-B230 Change a Circuit State" task on page 8-7.
- Apply to drop ports—Uncheck this check box.
  - Inter-domain (UCP) SLA—If the tunnel will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.

Step 6 Click **Next**.

Step 7 In the Circuit Source area, choose the node where the VT tunnel will originate from the Node drop-down menu.

Step 8 Click **Next**.

Step 9 In the Circuit Destination area, choose the node where the VT tunnel will terminate from the Node drop-down menu.

Step 10 Click **Next**.

Step 11 In the Circuit Routing Preferences area, uncheck **Route Automatically**.

Step 12 Click **Next**. In the Route Review and Edit area, node icons appear to route the tunnel. The circuit source node is selected. Green arrows pointing from the source node to other network nodes indicate spans that are available for routing the tunnel.

Step 13 Complete the "DLP-B219 Provision a VT Tunnel Route" task on page 5-32 for the tunnel you are creating. The Circuits window displays.

Step 14 Verify that the tunnel you just created appears in the circuits list. VT tunnels are identified by VTT in the Type column.

Stop. You have completed this procedure.

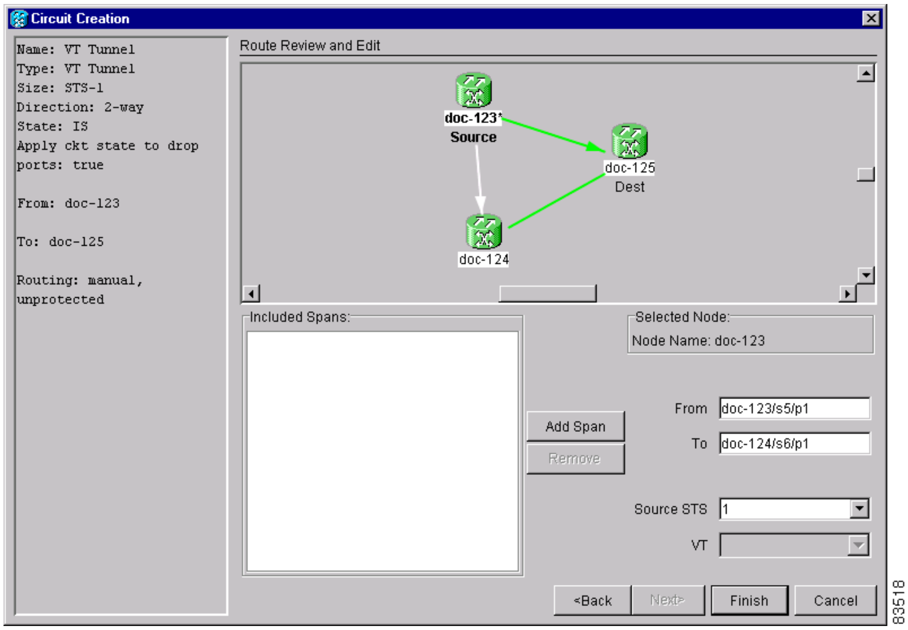
DLP-B219 Provision a VT Tunnel Route

Purpose	This task provisions the route for a manually-routed VT tunnel.
Tools/Equipment	None
Prerequisite Procedures	Perform this task as part of the "NTP-B134 Create a Manually Routed VT Tunnel" procedure on page 5-30.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 On the Circuit Creation wizard in the Route Review and Edit area, click the source node icon if it is not already selected. Arrows indicate the available spans for routing the tunnel from the source node.

Step 2 Click the arrow of the span you want the VT tunnel to travel. The arrow turns white. In the Selected Span area, the From and To fields display the slot and port that will carry the tunnel. The source STS appears. Figure 5-8 shows an example.

Figure 5-8 Manually Routing a VT Tunnel



Circuit Creation

Name: VT Tunnel
Type: VT Tunnel
Size: STS-1
Direction: 2-way
State: IS
Apply ckt state to drop ports: true

From: doc-123

To: doc-125

Routing: manual, unprotected

Route Review and Edit

Included Spans:

Selected Node:
Node Name: doc-123

From: doc-123/s5/p1
To: doc-124/s6/p1

Source STS: 1
VT:

Step 3 If you want to change the source STS, change it in the *Source STS* field; otherwise, continue with the next step.

Step 4 Click **Add Span**.The span is added to the Included Spans list and the span arrow turns blue.

Step 5 Repeat Steps 3 and 4 until the tunnel is provisioned from the source to the destination node through all intermediary nodes.

Step 6 Return to the "NTP-B134 Create a Manually Routed VT Tunnel" procedure on page 5-30.

NTP-B135 Test Electrical Circuits

Purpose	This procedure tests DS-1 and DS-3 circuits.
Tools/Equipment	A test set and all appropriate cables
Prerequisite Procedures	This procedure assumes you completed a facility loopback tests on the fibers and cables from the source and destination ONS 15327s to the DSX, and that you created a circuit using one of the following procedures: NTP-B181 Create an Automatically Routed DS-1 Circuit, page 5-5 NTP-B182 Create a Manually Routed DS-1 Circuit, page 5-9 NTP-B183 Create a Unidirectional DS-1 Circuit with Multiple Drops, page 5-11 NTP-B184 Create an Automatically Routed DS-3 Circuit, page 5-16 NTP-B185 Create a Manually Routed DS-3 Circuit, page 5-20 NTP-B186 Create a Unidirectional DS-3 Circuit with Multiple Drops, page 5-22
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at a node on the network where you created the circuit(s). If you are already logged in, continue with Step 2.

Step 2 From the View menu choose **Go to Network View**.

Step 3 Click the **Circuit** tab.

Step 4 Set the circuit and circuit ports to the maintenance state (OOS-MT). Take note of the original state because you will return the circuit to that state later.

- **a.** Click the circuit you want to test then choose **Circuits > Set Circuit State** from the Tools menu.
- **b.** On the Set Circuit State dialog box, choose **OOS-MT** from the Target State drop-down menu.
- **c.** Check the **Apply to drop ports** check box.
- **d.** Click **Apply**.

Step 5 Set the source and destination DS-1 port line length:

- **a.** In network view, double-click the source node.
- **b.** Double-click the circuit source XTC card and click the **Provisioning > Line** tabs.
- **c.** From the circuit source port Line Length drop-down menu choose the line length for the distance (in feet) between the DSX (if used) or circuit termination point and the source ONS 15327.
- **d.** Click **Apply**.
- **e.** From the View menu choose **Go to Network View**.
- **f.** Repeat Steps a. through e. for the destination port line length.

Step 6 Attach loopback cables to the circuit destination card.

- **a.** Verify the integrity of the loopback cable by looping the test set transmit (TX) connector to the test set receive (RX) connector. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before going to Step b.
- **b.** Attach the loopback cable to the port you are testing. Connect the transmit (TX) connector to the receive (RX) connector of the port.

Step 7 Attach loopback cables to the circuit source node.

a. Verify the integrity of loopback cable by looping the test set transmit (TX) connector to the test set receive (RX) connector. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly before going to Step b.

b. Attach the loopback cable to the port you are testing. Connect the test set to the circuit source port: transmit (TX) port of the test set to the circuit receive (RX) port; test set receive (RX) port to the circuit transmit (TX) port.

Step 8 Configure the test set for the ONS 15327 card that is the source of the circuit you are testing:

- DS-1—If you are testing an unmuxed DS-1, you must have a DSX-1 panel or a direct DS-1 interface into the ONS 15327. Set the test set for DS-1. For information about configuring your test set, consult your test set user guide.
- DS-3—If you are testing a clear channel DS-3, you must have a DSX-3 panel or a direct DS-3 interface into the ONS 15327. Set the test set for clear channel DS-3. For information about configuring your test set, consult your test set user guide.

Step 9 Verify that the test set displays a clean signal. If a clean signal is not displayed, repeat Steps 2 through 8 to make sure the test set and cabling is configured correctly.

Step 10 Inject errors from the test set. Verify that the errors display at the source and destination nodes.

Step 11 Clear the PMs for the ports that you tested. See the "DLP-B130 Clear Selected PM Counts" task on page 7-11 for instructions.

Step 12 Return the circuit and circuit ports to the state they were in at the beginning of the test:

a. Click the circuit you want to test then choose **Circuits > Set Circuit State** from the Tools menu.

b. In the Set Circuit State dialog box, choose **IS** (in service), **OOS** (out of service) or **OOS-AINS** (auto in service) from the Target State drop-down menu.

c. Check the **Apply to drop ports** check box.

d. Click **Apply**.

Step 13 Perform the protection switch test appropriate to the SONET topology:

- For UPSRs, complete the "DLP-B94 UPSR Protection Switching Test" task on page 4-25
- For BLSRs complete the "DLP-B91 BLSR Ring Switch Test" task on page 4-19.

Step 14 Perform a bit error rate test (BERT) for 12 hours or follow your site requirements for length of time. For information about configuring your test set for BERT, see your test set user guide.

Step 15 After the BERT is complete, print the results or save them to a disk for future reference. For information about printing or saving test results see your test set user guide.

Stop. You have completed this procedure.

NTP-B188 Create an Automatically Routed Optical Circuit

Purpose	This procedure creates an automatically-routed bidirectional or unidirectional optical circuit, including STS-1 and concatenated STS-3c, STS-6c, STS-9c, STS-12c, STS-24c, or STS-48c speeds.
Tools/Equipment	None
Prerequisite Procedures	NTP-B127 Verify Network Turn Up, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23at a node on the network where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the tunnel source and destination ports before you create the circuit, complete the "DLP-B314 Assign a Name to a Port" task on page 5-14. If not, continue with Step 3.

Step 3 From the View menu choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box (Figure 5-9 on page 5-36), complete the following fields:

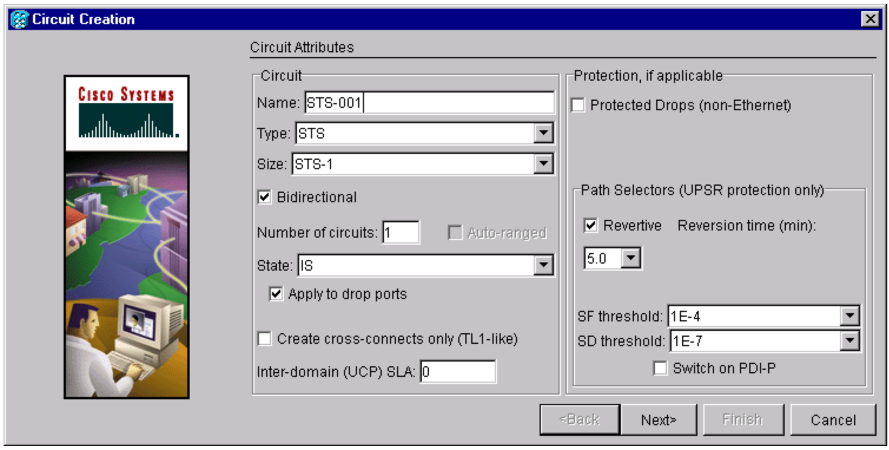
- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Type—Choose STS.
- Size—Choose the optical circuit size: STS-1, STS-3c, STS-6c, STS-9c, STS-12c, STS-24c, STS-48c.
- Bidirectional—Leave checked for this circuit.
- Number of circuits—Type the number of optical circuits you want to create. The default is 1. If you are creating multiple circuits with the same source and destination, you can use auto-ranging to create the circuits automatically.
- Auto-ranged—This check box is automatically checked when you enter more than 1 in the Number of circuits field. Leave checked if you are creating multiple optical circuits with the same source and destination and you want CTC to create the circuits automatically. Uncheck this check box if you do not want CTC to create the circuits automatically.
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and permits loopbacks on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-B230 Change a Circuit State" task on page 8-7.

- Apply to drop ports—Check this check box if you want to apply the state chosen in the State field to the circuit source and destination ports. CTC will apply the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the check box is unchecked, CTC will not change the state of the source and destination ports.

Note LOS alarms appear if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Check this check box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this box is checked, you cannot assign a name to the circuit. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Inter-domain (UCP) SLA—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Check this check box if you want the circuit routed to protected drops only, that is, to ONS 15327 cards that are in 1:1 or 1+1 protection. If you check this check box, CTC displays only protected cards as source and destination choices.

Figure 5-9 Setting Circuit Attributes for an Optical Circuit



Circuit Creation

Circuit Attributes

Circuit

Name: STS-001

Type: STS

Size: STS-1

☑ Bidirectional

Number of circuits: 1 □ Auto-ranged

State: IS

☑ Apply to drop ports

□ Create cross-connects only (TL1-like)

Inter-domain (UCP) SLA: 0

Protection, if applicable

□ Protected Drops (non-Ethernet)

Path Selectors (UPSR protection only)

☑ Revertive Reversion time (min): 5.0

SF threshold: 1E-4

SD threshold: 1E-7

□ Switch on PDI-P

Step 6 If the circuit will be routed on a UPSR, complete the "DLP-B218 Provision UPSR Selectors During Circuit Creation" task on page 5-25.

Step 7 Click **Next**.

Step 8 Complete the "DLP-B97 Provision an Optical Circuit Source and Destination" task on page 5-44 for the optical circuit you are creating.

Step 9 In the Circuit Routing Preferences area (Figure 5-10), choose **Route Automatically**. Two options are available; choose either, both, or none based on your preferences.

- Using Required Nodes/Spans—Check this check box to specify nodes and spans to include or exclude in the CTC-generated circuit route.
- Review Route Before Creation—Check this check box to review and edit the circuit route before the circuit is created.

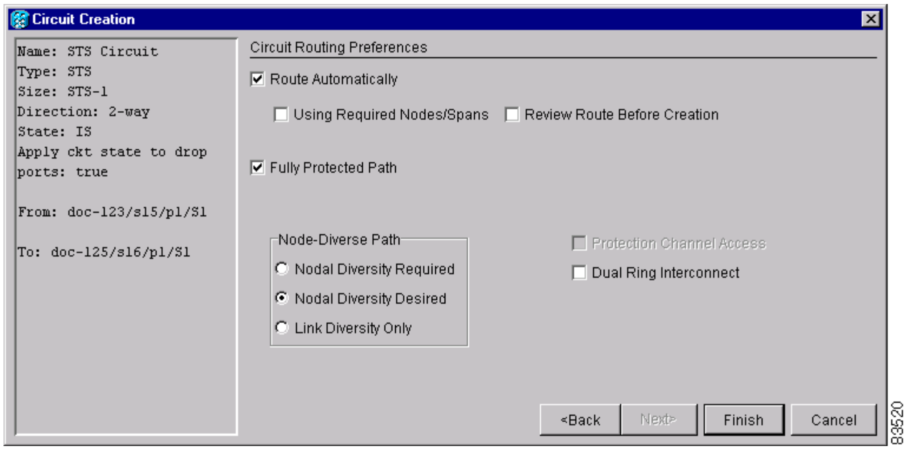
Step 10 Set the circuit path protection:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 11. CTC creates a fully-protected circuit route based on the path diversity option you choose. Fully-protected paths may or may not have UPSR path segments (with primary and alternate paths), and the path diversity options apply only to UPSR path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 12.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** on the Warning dialog box, and then continue with Step 12.

Step 11 If you selected Fully Protected Path, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within UPSR portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the UPSR portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for UPSR portions of the complete circuit path are needed. The paths may be node-diverse, but CTC does not check for node diversity.

Figure 5-10 Setting Circuit Routing Preferences for an Optical Circuit



Circuit Creation

```
Name: STS Circuit
Type: STS
Size: STS-1
Direction: 2-way
State: IS
Apply ckt state to drop
ports: true

From: doc-123/s15/p1/S1

To: doc-125/s16/p1/S1
```

Circuit Routing Preferences

☑ Route Automatically

□ Using Required Nodes/Spans □ Review Route Before Creation

☑ Fully Protected Path

Node-Diverse Path
○ Nodal Diversity Required
● Nodal Diversity Desired
○ Link Diversity Only

□ Protection Channel Access
□ Dual Ring Interconnect

Step 12 If you selected Using Required Nodes/Spans in Step 9, complete the following substeps. If not, continue with Step 13:

a. Click **Next**.

b. In the Circuit Route Constraints area, click a node or span on the circuit map.

c. Click **Include** to include the node or span in the circuit, or click **Exclude** to exclude the node or span from the circuit. The order in which you choose included nodes and spans is the order in which the circuit will be routed. Click spans twice to change the circuit direction.

d. Repeat Step c. for each node or span you wish to include or exclude.

e. Review the circuit route. To change the circuit routing order, choose a node in the Required Nodes/Lines or Excluded Notes Links lists, then click the **Up** or **Down** buttons to change the circuit routing order. Click **Remove** to remove a node or span.

Step 13 If you selected Review Route Before Creation in Step 9, complete the following substeps; otherwise, continue with Step 14:

a. Click **Next**.

b. Review the circuit route. To add or delete a circuit span, choose a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

c. If the provisioned circuit does not reflect the routing and configuration you want, click **Back** to verify and change circuit information. If the circuit needs to be routed to a different path, see the "NTP-B189 Create a Manually Routed Optical Circuit" procedure on page 5-38 to assign the circuit route yourself.

Step 14 Click **Finish**. One of the following results occurs, based on the circuit properties you provisioned in the Circuit Creation dialog box:

- If you entered more than 1 in Number of circuits and selected Auto-ranged, CTC automatically creates the number of circuits entered in Number of circuits. If auto ranging cannot complete all the circuits, for example, because sequential ports are unavailable on the source or destination, a dialog box appears. Set the new source or destination for the remaining circuits, then click **Finish** to continue auto ranging.
- If you entered more than 1 in Number of circuits and did not choose Auto-ranged, the Circuit Creation dialog box appears for you to create the remaining circuits. Repeat Steps Step 5 through 14 for each additional circuit.
- After completing the circuit(s), CTC displays the Circuits window.

Step 15 On the Circuits window, verify that the circuit(s) you created appear in the circuits list.

Step 16 Complete the "NTP-B62 Test Optical Circuits" procedure on page 5-46. Skip this step if you built a test circuit.

Stop. You have completed this procedure.

NTP-B189 Create a Manually Routed Optical Circuit

Purpose	This procedure creates a manually-routed, bidirectional or unidirectional optical circuit, including STS-1 and concatenated STS-3c, STS-6c, STS-9c, STS-12c, STS-24c, or STS-48c speeds.
Tools/Equipment	None
Prerequisite Procedures	NTP-B127 Verify Network Turn Up, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at a node on the network where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the tunnel source and destination ports before you create the circuit, complete the "DLP-B314 Assign a Name to a Port" task on page 5-14. If not, continue with Step 3.

Step 3 From the View menu choose **Go to Network View**.

Step 4 In the Circuit Creation dialog box, complete the following fields:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Type—Choose STS.
- Size—Choose the optical circuit size. Choices are STS-1, STS-3c, STS-6c, STS-9c, STS-12c, STS-24c, or STS-48c.
- Bidirectional—Leave checked for this circuit.
- Number of circuits—Type the number of optical circuits you want to create. The default is 1.
- Auto-ranged—Applies to automatically-routed circuits only. If you entered more than 1 in Number of Circuits, uncheck this check box. (The check box is unavailable if only one circuit is entered in Number of Circuits.)
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and permits loopbacks on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-B230 Change a Circuit State" task on page 8-7.
- Apply to drop ports—Check this check box if you want to apply the state chosen in the State field to the circuit source and destination ports. CTC will apply the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the check box is not checked, CTC will not change the state of the source and destination ports.

Note LOS alarms appear if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Check this check box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this box is checked, you cannot assign a name to the circuit. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Inter-domain (UCP) SLA—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Check this check box if you want the circuit routed to protect drops only, that is, to ONS 15327 cards that are in 1:1 or 1+1 protection. If you check this check box, CTC displays only protected cards as source and destination choices.

Step 5 If the circuit will be routed on a UPSR, set the UPSR path selectors. See the "DLP-B218 Provision UPSR Selectors During Circuit Creation" task on page 5-25.

Step 6 Click **Next**.

Step 7 Complete the "DLP-B97 Provision an Optical Circuit Source and Destination" task on page 5-44 for the optical circuit you are creating.

Step 8 In the Circuit Routing Preferences area (Figure 5-10 on page 5-37), uncheck **Route Automatically**.

Step 9 Set the circuit path protection:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 10.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 11.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** on the Warning dialog box, and then continue with Step 11.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 10 If you selected Fully Protected Path, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within the UPSR portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the UPSR portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for UPSR portions of the complete circuit path are needed. The paths may be node-diverse, but CTC does not check for node diversity.

Step 11 Click **Next**. In the Route Review and Edit area, node icons appear for you to route the circuit manually.

Step 12 Complete the "DLP-B98 Provision an Optical Circuit Route" task on page 5-45.

Step 13 Click **Finish**. If the path does not meet the specified path diversity requirement, CTC displays an error message and allows you to change the circuit path. If you entered more than 1 in Number of circuits, the Circuit Creation dialog box appears after the circuit is created for you to create the remaining circuits.

Step 14 Repeat Steps 4 through 13 for each additional circuit.

Step 15 When all the circuits are created, CTC displays the main Circuits window. Verify that the circuit(s) you created appear in the window.

Step 16 Complete the "NTP-B62 Test Optical Circuits" procedure on page 5-46.

Stop. You have completed this procedure.

NTP-B190 Create a Unidirectional Optical Circuit with Multiple Drops

Purpose	This procedure creates a unidirectional OC-N circuit with multiple traffic drops (circuit destinations)
Tools/Equipment	None
Prerequisite Procedures	NTP-B127 Verify Network Turn Up, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at a node on the network where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the tunnel source and destination ports before you create the circuit, complete the "DLP-B314 Assign a Name to a Port" task on page 5-14. If not, continue with Step 3.

Step 3 From the View menu choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

Step 5 In the Circuit Creation dialog box, complete the following fields:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Type—Choose STS.
- Size—Choose the circuit size: STS-1, STS-3c, STS-6c, STS-9c, STS-12c, STS-24c, or STS-48c.
- Bidirectional—Uncheck this check box for this circuit.
- Number of circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable when the Number of Circuits field is 1.
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and permits loopbacks on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-B230 Change a Circuit State" task on page 8-7.
- Apply to drop ports—Check this check box if you want to apply the state chosen in the State field to the circuit source and destination ports. CTC will apply the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the check box is not checked, CTC will not change the state of the source and destination ports.

Note LOS alarms appear if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Check this check box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this box is checked, you cannot assign a name to the circuit. Also, VT tunnels and Ethergroup sources and destinations are unavailable.
- Inter-domain (UCP) SLA—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Check this check box if you want the circuit routed to protect drops only, that is, to ONS 15327 cards that are in 1:1 or 1+1 protection. If you check this check box, CTC displays only protected cards as source and destination choices.

Step 6 If the circuit will be routed on a UPSR, set the UPSR path selectors. See the "DLP-B218 Provision UPSR Selectors During Circuit Creation" task on page 5-25.

Step 7 Click **Next**.

Step 8 Complete the "DLP-B97 Provision an Optical Circuit Source and Destination" task on page 5-44 for the circuit you are creating.

Step 9 Uncheck **Route Automatically**. When Route Automatically is not selected, Using Required Nodes/Spans and Review Route Before Circuit Creation are unavailable.

Step 10 Set the circuit path protection:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 11. Fully-protected paths may or may not have UPSR path segments (with primary and alternate paths), and the path diversity options apply only to UPSR path segments, if any exist.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 12.
- To route the circuit on a BLSR protection channel, if available, uncheck **Fully Protected Path**, check **Protection Channel Access**, click **Yes** on the Warning dialog box, and then continue with Step 12.

Caution Circuits routed on BLSR protection channels are not protected and are preempted during BLSR switches.

Step 11 If you selected Fully Protected Path, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within the UPSR portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the UPSR portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for UPSR portions of the complete circuit path are needed. The paths may be node-diverse, but CTC does not check for node diversity.

Note For manually-routed circuits, CTC checks your manually-provisioned path against the path diversity option you choose. If the path does not meet the path diversity requirement that is specified, CTC displays an error message.

Step 12 Click **Next**. In the Route Review and Edit area, node icons appear for you to route the circuit manually. The green arrows pointing from the selected node to other network nodes indicate spans that are available for routing the circuit.

Step 13 Complete the "DLP-B98 Provision an Optical Circuit Route" task on page 5-45.

Step 14 Click **Finish**. After completing the circuit, CTC displays the Circuits window.

Step 15 On the Circuits window, click the circuit that you want to route to multiple drops. The Delete, Edit, and Search buttons become active.

Step 16 Click **Edit**. The Edit Circuit window appears with the General tab selected. All nodes in the DCC network appear on the network. Circuit source and destination information appears under the source and destination nodes. To display a detailed view of the circuit, click **Show Detailed Map**. You can rearrange the node icons by selecting the node with the left mouse button, pressing **Ctrl** and dragging the icon to the new location.

Step 17 On the Edit Circuit dialog box, click the **Drops** tab. A list of existing drops appears.

Step 18 Click **Create**.

Step 19 On the Define New Drop dialog box, define the new drop:

a. Node—Choose the target node for the circuit drop.

b. Slot—Choose the target card and slot.

c. Port, STS—Choose the port and/or STS from the Port and STS drop-down menus. The choice in these menus depends on the card selected in Step b. See Table 5-2 on page 5-2 for a list of options.

d. The routing preferences for the new drop will match those of the original circuit. However, you can modify the following:

- If the original circuit was routed on a protected path, you can change the nodal diversity options: Required, Desired, Don't Care; Link Diverse only. See Step 11 for options descriptions.
- If the original circuit was not routed on a protected path, the Protection Channel Access options is available. See Step 12 for a description of the PCA option.

e. Click **OK**. The new drop appears in the Drops list.

Step 20 If you need to create additional drops on the circuit, repeat Steps 17 through 19.

Step 21 Click **Close**. The Circuits window appears.

Step 22 Verify that the new drops appear in the Destination column for the circuit you edited. If they do not appear, repeat Steps 18 through 21 making sure all options are provisioned correctly.

Step 23 Complete the "NTP-B62 Test Optical Circuits" procedure on page 5-46.

Stop. You have completed this procedure.

DLP-B97 Provision an Optical Circuit Source and Destination

Purpose	This task provisions the source and destination cards for an optical circuit.
Tools/Equipment	None
Prerequisite Procedures	Perform this task during one of the following procedures: NTP-B188 Create an Automatically Routed Optical Circuit, page 5-35 NTP-B189 Create a Manually Routed Optical Circuit, page 5-38 NTP-B190 Create a Unidirectional Optical Circuit with Multiple Drops, page 5-41
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Node drop-down menu choose the node where the circuit will originate.

Step 2 From the Slot drop-down menu choose the slot containing the optical card where the circuit originates. (If a card's capacity is fully utilized, it does not appear in the menu.)

Step 3 Depending on the circuit origination card, choose the source port and/or STS from the Port and STS sub-menus. The Port menu is only available if the card has multiple ports. STSs are not displayed if they are already in use by other circuits.

Note The STSs that display depend on the card, circuit size, and protection scheme. For example, if you create an STS-3c circuit on an OC-12 card in a UPSR, only four STSs are available. If you create an STS-3c circuit on an OC-12 card in a BLSR, two STSs are available because of the BLSR protection characteristics.

Step 4 If you need to create a secondary source, for example, a UPSR bridge/selector circuit entry point in a multivendor UPSR, click **Use Secondary Source** and repeat Steps 1 through 3 to define the secondary source.

Step 5 Click **Next**.

Step 6 From the Node drop-down menu choose the destination node.

Step 7 From the Slot drop-down menu choose the slot containing the optical card where the circuit will terminate (destination card). (If a card's capacity is fully utilized, the card does not appear in the menu.)

Step 8 Depending on the card selected in Step 2, choose the destination port and/or STS from the Port and STS sub-menus. The Port menu is available only if the card has multiple ports. The STSs that display depend on the card, circuit size, and protection scheme.

Step 9 If you need to create a secondary destination, for example, a UPSR bridge/selector circuit entry point in a multivendor UPSR, click **Use Secondary Destination** and repeat Steps 6 through 8 to define the secondary destination.

Step 10 Click **Next**.

Step 11 Return to your originating procedure (NTP).

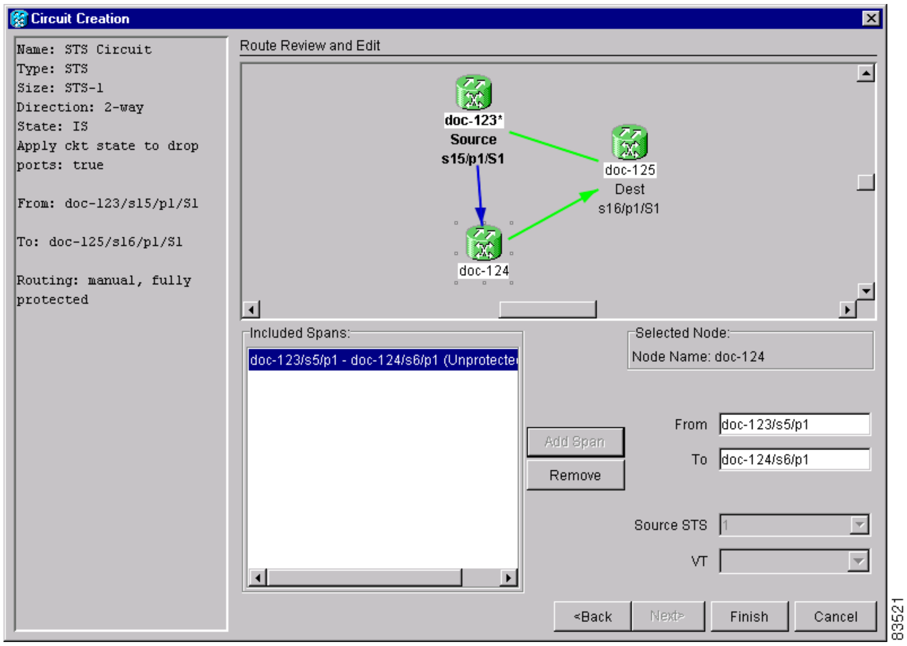
DLP-B98 Provision an Optical Circuit Route

Purpose	This task provisions an optical circuit route for manually-routed circuits.
Tools/Equipment	None
Prerequisite Procedures	Perform this task during one of the following procedures: NTP-B188 Create an Automatically Routed Optical Circuit, page 5-35 NTP-B189 Create a Manually Routed Optical Circuit, page 5-38 NTP-B190 Create a Unidirectional Optical Circuit with Multiple Drops, page 5-41
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 On the Circuit Creation wizard in the Route Review and Edit area, click the source node icon if it is not already selected.

Step 2 Starting with a span on the source node, click the arrow of the span you want the circuit to travel. The arrow turns white. In the Selected Span area, the From and To fields display span information. The source STS appears. Figure 5-11 shows an example.

Figure 5-11 Manually Routing an OC-N Circuit



Circuit Creation

Name: STS Circuit
Type: STS
Size: STS-1
Direction: 2-way
State: IS
Apply ckt state to drop ports: true

From: doc-123/s15/p1/S1

To: doc-125/s16/p1/S1

Routing: manual, fully protected

Included Spans:
doc-123/s5/p1 - doc-124/s6/p1 (Unprotecte

Selected Node:
Node Name: doc-124

From: doc-123/s5/p1
To: doc-124/s6/p1
Source STS: 1
VT:

Step 3 If you want to change the source STS, adjust the Source STS field; otherwise, continue with the next step.

Note VT is gray for OC-N circuits.

Step 4 Click **Add Span**.The span is added to the Included Spans list and the span arrow turns blue.

Step 5 Repeat Steps 2 through 4 until the circuit is provisioned from the source to the destination node through all intermediary nodes. If Fully Protect Path is checked on the Circuit Routing Preferences panel, you must:

- Add two spans for all UPSR or unprotected portions of the circuit route from the source to the destination
- Add one span for all BLSR or 1+1 portions of route from the source to the destination

Suppose you want to create a fully protected circuit from a UPSR node subtended from the BLSR. For example, a BLSR is comprised of Node 1, Node 2, and Node 3, and a UPSR subtends from Node 3 to Node 4. To create a circuit from Node 4 to Node 1, you include two spans in the circuit route from Node 4 to Node 3, since both the working and protect path must be provisioned for the UPSR portion of the circuit, and you provision one circuit span from Node 3 to Node 1, since the BLSR provides protection.

Step 6 Return to your originating procedure (NTP).

NTP-B62 Test Optical Circuits

Purpose	This procedure tests an optical circuit.
Tools/Equipment	Test set capable of optical speeds, appropriate fibers, and attenuators
Prerequisite Procedures	This procedure assumes you completed facility loopback tests to test the fibers and cables from the source and destination ONS 15327s to the fiber distribution panel or the DSX and one of following circuit procedures: NTP-B188 Create an Automatically Routed Optical Circuit, page 5-35 NTP-B189 Create a Manually Routed Optical Circuit, page 5-38
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note If this has not been done, do so now before completing the optical circuit test procedure.

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at a node on the network where you created the circuit(s). If you are already logged in, continue with Step 2.

Step 2 From the View menu choose **Go to Network View**.

Step 3 Click the **Circuits** tab.

Step 4 Set the circuit and circuit ports to Out of Service-Maintenance (OOS_MT):

a. Click the circuit you want to test.

b. From the Tools menu choose **Circuits > Set Circuit State**.

c. In the Set Circuit State dialog box, choose **OOS-MT** from the Target State drop-down menu.

d. If it is unchecked, check the **Apply to drop ports** check box.

e. Click **Apply**.

Step 5 Set up the patch cable at the destination node:

a. Test the patch cable by connecting one end to the test set transmit (TX) port and the other end to the test receive (RX) port. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly.

b. Install the loopback cable on the port you are testing. Connect the transmit (TX) to the receive (RX) of the port being tested.

Step 6 Set up the loopback cable at the source node:

a. Test the loopback cable by connecting one end to the test set transmit (TX) port and the other end to the test receive (RX) port. If the test set does not run error-free, check the cable for damage and check the test set to make sure it is set up correctly.

b. At the source node attach the loopback cable to the port you are testing. Connect the test set to the circuit source port: transmit (TX) port of the test set to the circuit receive (RX) port; test set receive (RX) port to the circuit transmit (TX) port.

Step 7 Configure the test set for the source ONS 15327 card:

- OC-3 cards—You will test either an OC-3c (the “c” denotes concatenated) or a muxed OC-3. If you are testing an OC-3c, configure the test set for an OC-3c. If you are testing a muxed OC-3, configure the test set for a muxed OC-3 and choose the DS-3 and/or DS-1 you will test. For information about configuring your test set, consult your test set user guide.
- OC-12 cards—You will test either an OC-12c or a muxed OC-12. If you are testing an OC-12c, configure the test set for an OC-12c. If you are testing a muxed OC-12, configure the test set for a muxed OC12 and choose the DS-3 and/or DS-1 you will test. For information about configuring your test set, consult your test set user guide.
- OC-48 cards—You will test either an OC-48c or a muxed OC-48. If you are testing an OC-48c configure the test set for an OC-48c. If you are testing a muxed OC-48, configure the test set for a muxed OC-48 and choose the DS-3 and/or DS-1 you will test. For information about configuring your test set, consult your test set user guide.

Step 8 Verify that the test set displays a clean signal. If a clean signal is not displayed, repeat Steps 2 through 7 to make sure you have configured the test set and cabling.

Step 9 Inject errors from the test set. Verify that the errors display at the source and destination nodes.

Step 10 Clear the PMs for the ports that you tested. See the “DLP-B130 Clear Selected PM Counts” task on page 7-11 for instructions.

Step 11 Perform protection switch testing appropriate to SONET topology:

- For UPSRs, see the “DLP-B94 UPSR Protection Switching Test” task on page 4-25.
- For BLSRs see the “DLP-B91 BLSR Ring Switch Test” task on page 4-19.

Step 12 Perform a bit error rate test (BERT) for 12 hours or a duration dictated by local testing custom. For information about configuring your test set for BERT, see your test set user guide.

Step 13 After the BERT is complete, print the results or save them to a disk for future reference. For information about printing or saving test results see your test set user guide.

Step 14 Change the circuit and circuit ports from OOS_MT to their previous service states:

a. Click the circuit you want to test then, from the Tools menu choose **Circuits > Set Circuit State**.

b. On the Set Circuit State dialog box, choose **IS** (in service), **OOS**, (out of service) or **OOS-AINS** (auto inservice) from the Target State drop-down menu.

c. If it is unchecked, check the **Apply to drop ports** check box.

d. Click **Apply**.

Stop. You have completed this procedure.

NTP-B191 Create an E-Series EtherSwitch Circuit (Multicard or Single-Card Mode)

Purpose	This procedure creates a multicard or single-card EtherSwitch circuit. It does not apply to E-Series cards in port-mapped mode. To create a port-mapped mode circuit, see the NTP-B192 Create a Circuit for an E-Series Card in Port-Mapped Mode, page 5-50.
Tools/Equipment	E-Series Ethernet cards must be installed at each end of the Ethernet circuit.
Prerequisite Procedures	NTP-B127 Verify Network Turn Up, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at a node on the network where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If a high number of VLANs is already used by the network, complete the "DLP-B99 Determine Available VLANs" task on page 5-63 to verify that sufficient VLAN capacity is available (you will create a VLAN during each circuit creation task).

Step 3 Verify that the circuit source and destination Ethernet cards are provisioned for the mode of the circuit you will create, either multicard or single-card. See the "DLP-B246 Provision E-Series Ethernet Card Mode" task on page 5-64.

Step 4 Provision and enable the Ethernet ports. See "DLP-B220 Provision E-Series Ethernet Ports" task on page 5-64.

Step 5 From the View menu choose **Go to Network View**.

Step 6 Click the **Circuits** tab, then click **Create**.

Step 7 In the Create Circuits dialog box, complete the following fields:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Type—Choose STS.
- Size—Choose the circuit size. Valid circuit sizes for an Ethernet multicard circuit are STS-1 and STS-3c. Valid circuit sizes for an Ethernet single-card circuit are STS-1, STS-3c, STS6c, and STS12c.
- Bidirectional—Leave the default unchanged (checked).
- Number of circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable.
- State—Choose IS (in service). Ethergroup circuits are always in service.

- Apply to drop ports—Uncheck this check box.
- Create cross-connects only (TL1-like)—Uncheck this check box; it does not apply to Ethernet circuits.
- Inter-domain (UCP) SLA—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Leave the default unchanged (unchecked).

Step 8 If the circuit will be routed on a UPSR, complete the "DLP-B218 Provision UPSR Selectors During Circuit Creation" task on page 5-25.

Step 9 Click **Next**.

Step 10 Provision the circuit source:

a. From the Node drop-down menu choose one of the EtherSwitch circuit endpoint nodes. Either end node can be the EtherSwitch circuit source.

b. From the Slot drop-down menu choose one of the following:

   - If you are building a multicard EtherSwitch circuit, choose **Ethergroup**.
   - If you are building a single-card EtherSwitch circuit, choose the Ethernet card where you enabled the single-card EtherSwitch.

Step 11 Click **Next**.

Step 12 Provision the circuit destination:

a. From the Node drop-down menu choose the second EtherSwitch circuit endpoint node.

b. From the Slot drop-down menu choose one of the following:

   - If you are building a multicard EtherSwitch circuit, choose **Ethergroup**.
   - If you are building a Single-card EtherSwitch circuit, choose the Ethernet card where you enabled the single-card EtherSwitch.

Step 13 Click **Next**.

Step 14 In the Circuit VLAN Selection area, click **New VLAN**. If the desired VLAN already exists, continue with Step 17.

Step 15 In the New VLAN dialog box, complete the following:

- VLAN Name—Assign an easily-identifiable name to your VLAN.
- VLAN ID—Assign a VLAN ID. The VLAN ID should be the next available number between 2 and 4093 that is not already assigned to an existing VLAN. Each ONS 15327 network supports a maximum of 509 user-provisionable VLANs.

Step 16 Click **OK**.

Step 17 In the Circuit VLAN Selection area, highlight the VLAN name and click the arrow button (>>) to move the available VLAN(s) to the Circuit VLANs column.

Step 18 If you are building a single-card EtherSwitch circuit and want to disable spanning tree protection on this circuit, uncheck the **Enable Spanning Tree** check box and click **OK** on the Disabling Spanning Tree dialog box. The Enable Spanning Tree check box will remain checked or unchecked for the creation of the next single-card point-to-point Ethernet circuits.

⚠ **Caution** Disabling spanning tree protection increases the likelihood of logic loops on an Ethernet network.

Caution Turning off spanning tree on a circuit-by-circuit basis means that the ONS 15327 is no longer protecting the Ethernet circuit and that the circuit must be protected by another mechanism in the Ethernet network.

Caution Multiple circuits with spanning tree protection enabled will incur blocking if the circuits traverse the same E-series card and use the same VLAN.

Note You can disable or enable spanning tree protection on a circuit-by-circuit basis only for single-card, point-to-point Ethernet circuits. Other E-series Ethernet configurations disable or enable spanning tree on a port-by-port basis.

Step 19 Click **Next**.

Step 20 Confirm that the following information about the circuit is correct:

- Circuit name
- Circuit type
- Circuit size
- ONS 15327 circuit nodes

Step 21 Click **Finish**.

Step 22 Complete the "DLP-B220 Provision E-Series Ethernet Ports" task on page 5-64.

Step 23 Complete the "DLP-B221 Provision E-Series Ethernet Ports for VLAN Membership" task on page 5-65.

Stop. You have completed this procedure.

NTP-B192 Create a Circuit for an E-Series Card in Port-Mapped Mode

Purpose	This procedure creates an E-Series point-to-point SONET circuit with an E-Series card in port-mapped mode.
Tools/Equipment	An E-Series Ethernet card must be installed at each end of the circuit and configured in port-mapped mode.
Prerequisite Procedures	NTP-B127 Verify Network Turn Up, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at a node on the network where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 Provision the Ethernet cards that will carry the circuit for port-mapped mode. See the "DLP-B246 Provision E-Series Ethernet Card Mode" task on page 5-64.

Step 3 Provision and enable the Ethernet ports. See the "DLP-B220 Provision E-Series Ethernet Ports" task on page 5-64.

Step 4 From the View menu choose **Go to Network View**.

Step 5 Click the **Circuits** tab and click **Create**.

Step 6 In the Create Circuits dialog box, complete the following fields:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Type—Choose STS.
- Size—Choose the circuit size. Valid circuit sizes for an E-Series circuit in port-mapped mode are STS-1, STS-3c, STS6c, STS-9c, and STS-12c.
- Bidirectional—Leave the default unchanged (checked).
- Number of circuits—Leave the default unchanged (1).
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and permits loopbacks on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-B230 Change a Circuit State" task on page 8-7.
- Apply to drop ports—Select this checkbox if you want to apply the state chosen in the State field (IS or OOS-MT only) to the Ethernet circuit source and destination ports. You cannot apply OOS-AINS to E-Series Ethernet card ports. CTC will apply the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the drop port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the check box is unchecked, CTC will not change the state of the source and destination ports.

Note LOS alarms appear if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Uncheck this check box.
- Inter-domain (UCP) SLA—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Auto-ranged—Unavailable.
- Protected Drops—Leave the default unchanged (unchecked).

Step 7 If the circuit will be routed on a UPSR, complete the "DLP-B218 Provision UPSR Selectors During Circuit Creation" task on page 5-25.

Step 8 Click **Next**.

Step 9 Provision the circuit source:

a. From the Node drop-down menu choose the circuit source node. Either end node can be the point-to-point circuit source.

b. From the Slot drop-down menu choose the slot containing the E-Series card that you will use for one end of the point-to-point circuit.

c. From the Port drop-down menu choose a port.

Step 10 Click **Next**.

Step 11 Provision the circuit destination:

a. From the Node drop-down menu choose the circuit destination node.

b. From the Slot drop-down menu choose the slot containing the E-Series card that you will use for other end of the point-to-point circuit.

c. From the Port drop-down menu choose a port.

Step 12 Click **Next**. The Circuits window appears.

Step 13 Confirm that the following circuit information is correct:

- Circuit name
- Circuit type
- Circuit size
- ONS 15327 circuit nodes

Step 14 Click **Finish**.

Step 15 Complete the "NTP-B146 Test E-Series Circuits" procedure on page 5-67.

Stop. You have completed this procedure.

NTP-B142 Create an E-Series Shared Packet Ring Ethernet Circuit

Purpose	This procedure creates a shared packet ring Ethernet circuit. It does not apply to E-Series cards in port-mapped mode.
Tools/Equipment	E-Series Ethernet cards must be installed at both Ethernet circuit endpoint nodes.
Prerequisite Procedures	NTP-B127 Verify Network Turn Up, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at a node on the network where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If a high number of VLANs is already used by the network, complete the "DLP-B99 Determine Available VLANs" task on page 5-63 to verify that sufficient VLAN capacity is available (you will create a VLAN during each circuit creation task).

Step 3 Verify that the Ethernet cards that will carry the circuit are provisioned for multi-card EtherSwitch Group. See the "DLP-B246 Provision E-Series Ethernet Card Mode" task on page 5-64.

Step 4 Provision and enable the Ethernet ports. See "DLP-B220 Provision E-Series Ethernet Ports" task on page 5-64.

Step 5 From the View menu choose **Go to Network View**.

Step 6 Click the **Circuits** tab and click **Create**.

Step 7 In the Create Circuits dialog box, complete the following fields:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Type—Choose STS.
- Size—Choose the circuit size. Valid shared packet ring circuit sizes are STS-1 and STS-3c.
- Bidirectional—Leave the default unchanged (checked).
- Number of circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable.
- State—Choose **IS** (in service). Ethergroup circuits are always in service.
- Apply to drop ports—Uncheck this check box; states cannot be applied to E-Series ports.
- Create cross-connects only (TL1-like)—Uncheck this check box; it does not apply to Ethernet circuits.
- Inter-domain (UCP) SLA—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Leave the default unchanged (unchecked).

Step 8 If the circuit will be routed on a UPSR, complete the "DLP-B218 Provision UPSR Selectors During Circuit Creation" task on page 5-25.

Step 9 Click **Next**.

Step 10 Provision the circuit source:

a. From the Node drop-down menu choose one of the shared packet ring circuit endpoint nodes. Either end node can be the shared packet ring circuit source.

b. From the Slot drop-down menu choose **Ethergroup**.

Step 11 Click **Next**.

Step 12 Provision the circuit destination:

a. From the Node drop-down menu choose the second shared packet ring circuit endpoint node.

b. From the Slot drop-down menu choose **Ethergroup**.

Step 13 Click **Next**.

Step 14 Review the VLANs listed in the Available VLANs area. If the VLAN you want to use appears, continue with Step 15. If you need to create a new VLAN, complete the following steps:

a. Click the **New VLAN** button.

b. On the New VLAN dialog box, complete the following:

- VLAN Name—Assign an easily-identifiable name to your VLAN.
- VLAN ID—Assign a VLAN ID. The VLAN ID should be the next available number between 2 and 4093 that is not already assigned to an existing VLAN. Each ONS 15327 network supports a maximum of 509 user-provisionable VLANs.

c. Click **OK**.

Step 15 In the Available VLANs column, click the VLAN you want to use and click the arrow button (>>) to move the VLAN to the Circuit VLANs column.

Note Moving the VLAN from Available VLANs to Circuit VLANs forces all the VLAN traffic to use the shared packet ring you are creating.

Step 16 Click **Next**.

Step 17 In the Circuit Routing Preferences area, uncheck the **Route Automatically** check box and click **Next**.

Step 18 In the Route Review and Edit area, click the source node, then click a span (green arrow) that is leading away from the source node.

The span turns white.

Step 19 Click **Add Span**.

The span turns blue. CTC adds the span to the Included Spans list.

Step 20 Click the node at the end of the blue span.

Step 21 Click the green span attached to the node selected in Step 20.

The span turns white.

Step 22 Click **Add Span**.

The span turns blue.

Step 23 Repeat Steps 19 through 22 for every node in the ring.

Step 24 Verify that the new circuit is correctly configured. If the circuit information is not correct, click the **Back** button and repeat the procedure with the correct information.

Note If the circuit is incorrect, you can also click **Finish**, delete the completed circuit, and begin the procedure again.

Step 25 Click **Finish**.

Step 26 Complete the "DLP-B220 Provision E-Series Ethernet Ports" task on page 5-64 for each node that carries the circuit.

Step 27 Complete the "DLP-B221 Provision E-Series Ethernet Ports for VLAN Membership" task on page 5-65 for each node that carries the circuit.

Step 28 Complete the "NTP-B146 Test E-Series Circuits" procedure on page 5-67.

Stop. You have completed this procedure.

NTP-B143 Create an E-Series Hub and Spoke Ethernet Configuration

Purpose	This procedure creates a hub and spoke Ethernet configuration, which is made up of multiple circuits that share a common endpoint. It does not apply to E-Series cards in port-mapped mode.
Tools/Equipment	E-Series Ethernet cards must be installed at all Ethernet circuit endpoint nodes.
Prerequisite Procedures	NTP-B127 Verify Network Turn Up, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at the hub node (common endpoint). If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-B99 Determine Available VLANs" task on page 5-63 to verify that sufficient VLAN capacity is available (you will create a VLAN during each circuit creation task).

Step 3 Display the node view.

Step 4 Verify that the Ethernet card that will carry the hub and spoke circuit is provisioned for Single-card EtherSwitch Group. See the "DLP-B246 Provision E-Series Ethernet Card Mode" task on page 5-64.

Step 5 Provision and enable the Ethernet ports. See "DLP-B220 Provision E-Series Ethernet Ports" task on page 5-64.

Step 6 Log into the destination spoke node, and repeat Steps 3 and 4 for the destination Ethernet card. You only need to verify that the hub node is provisioned for single-card EtherSwitch once.

Step 7 Click the **Circuits** tab and click **Create**.

Step 8 In the Create Circuits dialog box, complete the following fields:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Type—Choose STS.
- Size—Choose the circuit size. Valid circuit sizes for an Ethernet single-card circuit are STS-1, STS-3c, STS6c, and STS12c.
- Bidirectional—Leave the default unchanged (checked).
- Number of circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable.
- State—Choose IS (in service)
- Apply to drop ports—Uncheck this check box; states cannot be applied to E-Series ports.
- Create cross-connects only (TL1-like)—uncheck this check box; it does not apply to Ethernet circuits.
- Inter-domain (UCP) SLA—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.

- Protected Drops—Leave the default unchanged (unchecked).

Step 9 If the circuit will be routed on a UPSR, complete the "DLP-B218 Provision UPSR Selectors During Circuit Creation" task on page 5-25.

Step 10 Click **Next**.

Step 11 Provision the circuit source:

a. From the Node drop-down menu choose the hub node.

b. From the Slot drop-down menu choose the Ethernet card where you enabled the single-card EtherSwitch.

Step 12 Click **Next**.

Step 13 Provision the circuit destination:

a. From the Node drop-down menu choose an EtherSwitch circuit endpoint node.

b. From the Slot drop-down menu choose the Ethernet card where you enabled the single-card EtherSwitch.

Step 14 Click **Next**.

Step 15 Review the VLANs listed in the Available VLANs area. If the VLAN you want to use appears, continue with Step 17. If you need to create a new VLAN, complete the following steps:

a. Click the **New VLAN** button.

b. On the New VLAN dialog box, complete the following:

- VLAN Name—Assign an easily-identifiable name to your VLAN.
- VLAN ID—Assign a VLAN ID. The VLAN ID should be the next available number between 2 and 4093 that is not already assigned to an existing VLAN. Each ONS 15327 network supports a maximum of 509 user-provisionable VLANs.

c. Click **OK**.

Step 16 In the Available VLANs column, click the VLAN you want to use and click the arrow button (**>>**) to move the VLAN to the Circuit VLANs column.

Note Moving the VLAN from Available VLANs to Circuit VLANs forces all the VLAN traffic to use the shared packet ring you are creating.

Step 17 Click **Next**.

Step 18 Confirm that the following information about the hub and spoke circuit is correct:

- Circuit name
- Circuit type
- Circuit size
- VLAN names
- ONS 15327 circuit nodes

If the circuit information is not correct, click the **Back** button and repeat the procedure with the correct information.

Note You can also click **Finish**, delete the completed circuit, and start the procedure from the beginning.

Step 19 Click **Finish**.

Step 20 Complete the "DLP-B220 Provision E-Series Ethernet Ports" task on page 5-64.

Step 21 Complete the "DLP-B221 Provision E-Series Ethernet Ports for VLAN Membership" task on page 5-65.

Step 22 Complete the "NTP-B146 Test E-Series Circuits" procedure on page 5-67.

Step 23 To create additional circuits ("spokes"):

a. Complete the "DLP-B99 Determine Available VLANs" task on page 5-63 to verify that sufficient VLAN capacity is available for the circuit destination node.

b. Repeat Steps 3 through 22.

Stop. You have completed this procedure.

NTP-B144 Create an E-Series Single-Card EtherSwitch Manual Cross-Connect

Purpose	This procedure creates Single-Card EtherSwitch cross-connects between E-Series Ethernet cards and OC-N cards connected to non-ONS equipment.
Tools/Equipment	E-Series Ethernet cards must be installed at the circuit source node.
Prerequisite Procedures	NTP-B127 Verify Network Turn Up, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note In this procedure, cross-connect refers to a circuit connection created within the same node between the Ethernet card and an OC-N card connected to third-party equipment. You create cross-connects at the source and destination nodes so an Ethernet circuit can be routed from source to destination across third-party equipment.

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at a node on the network where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, complete the "DLP-B314 Assign a Name to a Port" task on page 5-14. If not, continue with Step 3.

Step 3 If a high number of VLANs is already used by the network, complete the "DLP-B99 Determine Available VLANs" task on page 5-63 to verify that sufficient VLAN capacity is available (you will create a VLAN during each circuit creation task).

Step 4 Verify that the Ethernet card that will carry the circuit is provisioned for Singlecard EtherSwitch. See the "DLP-B246 Provision E-Series Ethernet Card Mode" task on page 5-64.

Step 5 From the View menu choose **Go to Network View**.

Step 6 Click the **Circuits** tab and click **Create**.

Step 7 In the Create Circuits dialog box, complete the following fields:

- Name—Assign a name to the cross-connect. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the cross-connect.
- Type—Choose STS.
- Size—Choose the cross-connect size. For single-card EtherSwitch, the available sizes are STS-1, STS-3c, STS-6c, and STS-12c.
- Bidirectional—Leave the default unchanged (checked).
- Number of circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable.
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS— The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and permits loopbacks on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-B230 Change a Circuit State" task on page 8-7.
- Apply to drop ports—Uncheck this check box.
- Create cross-connects only (TL1-like)—Uncheck this check box.
- Inter-domain (UCP) SLA—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Leave the default unchanged (unchecked).

Step 8 If the circuit will be routed on a UPSR, complete the "DLP-B218 Provision UPSR Selectors During Circuit Creation" task on page 5-25.

Step 9 Click **Next**.

Step 10 Provision the circuit source:

a. From the Node drop-down menu choose the cross-connect source node.

b. From the Slot drop-down menu choose the Ethernet card where you enabled the single-card EtherSwitch.

Step 11 Click **Next**.

Step 12 Provision the circuit destination:

a. From the Node drop-down menu choose the cross-connect circuit source node selected in Step 8. (For Ethernet cross-connects, the source and destination nodes are the same.)

b. From the Slot drop-down menu choose the OC-N card that is connected to the non-ONS equipment.

c. Depending on the OC-N card, choose the port and/or STS from the Port and STS drop-down menus.

Step 13 Click **Next**.

Step 14 Review the VLANs listed in the Available VLANs area. If the VLAN you want to use appears, continue with Step 15. If you need to create a new VLAN, complete the following steps:

a. Click the **New VLAN** button.

b. On the New VLAN dialog box, complete the following:

- VLAN Name—Assign an easily-identifiable name to your VLAN.
- VLAN ID—Assign a VLAN ID. The VLAN ID should be the next available number between 2 and 4093 that is not already assigned to an existing VLAN. Each ONS 15327 network supports a maximum of 509 user-provisionable VLANs.

c. Click **OK**.

Step 15 Click the VLAN you want to use on the Available VLANs column, then click the arrow **>>** button to move the VLAN to the Circuit VLANs column.

Step 16 Click **Next**. The Circuit Creation (Circuit Routing Preferences) dialog box opens.

Step 17 Confirm that the following information about the single-card EtherSwitch manual cross-connect is correct (in this task, “circuit” refers to the Ethernet cross-connect):

- Circuit name
- Circuit type
- Circuit size
- VLAN names
- ONS 15327 nodes

If the information is not correct, click the **Back** button and repeat the procedure with the correct information.

Step 18 Click **Finish**.

Step 19 Complete the “DLP-B220 Provision E-Series Ethernet Ports” task on page 5-64.

Step 20 Complete the “DLP-B221 Provision E-Series Ethernet Ports for VLAN Membership” task on page 5-65.

Stop. You have completed this procedure.

NTP-B145 Create an E-Series Multicard EtherSwitch Manual Cross-Connect

Purpose	This procedure manually creates Multicard EtherSwitch cross-connects between E-Series Ethernet cards and OC-N cards connected to non-ONS equipment.
Tools/Equipment	E-Series Ethernet cards must be installed at the circuit source node.
Prerequisite Procedures	NTP-B127 Verify Network Turn Up, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note In this procedure, cross-connect refers to a circuit connection created within the same node between the Ethernet card and an OC-N card connected to third-party equipment. You create cross-connects at the source and destination nodes so an Ethernet circuit can be routed from source to destination across third-party equipment.

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at a circuit endpoint. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-B99 Determine Available VLANs" task on page 5-63 to verify that sufficient VLAN capacity is available (you will create a VLAN during each circuit creation task).

Step 3 Verify that the Ethernet card that will carry the circuit is provisioned for Multicard EtherSwitch Group. See the "DLP-B246 Provision E-Series Ethernet Card Mode" task on page 5-64.

Step 4 Provision and enable the Ethernet ports. See "DLP-B220 Provision E-Series Ethernet Ports" task on page 5-64.

Step 5 From the View menu choose **Go to Network View**.

Step 6 Click the **Circuits** tab and click **Create**.

Step 7 In the Create Circuits dialog box, complete the following fields:

- Name—Assign a name to the source cross-connect. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the source cross-connect.
- Type—Choose STS.
- Size—Choose the size of the circuit that will be carried by the cross-connect. For multicard EtherSwitch circuits, the available sizes are STS-1 and STS-3c.
- Bidirectional—Leave checked.
- Number of circuits—Leave the default unchanged (1).
- Auto-ranged—Unavailable.
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.

  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and permits loopbacks on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-B230 Change a Circuit State" task on page 8-7.
- Apply to drop ports—Uncheck this check box.
- Create cross-connects only (TL1-like)—Uncheck this check box.
- Inter-domain (UCP) SLA—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Leave the default unchanged (unchecked).

Step 8 If the circuit will be routed on a UPSR, complete the "DLP-B218 Provision UPSR Selectors During Circuit Creation" task on page 5-25.

Step 9 Click **Next**.

Step 10 Provision the cross-connect source:

a. From the Node drop-down menu choose the cross-connect source node.

b. From the Slot drop-down menu choose **Ethergroup**.

Step 11 Click **Next**.

Step 12 From the Node drop-down menu in the Destination area, choose the circuit source node selected in Step 10. For Ethernet cross-connects, the source and destination nodes are the same.

The Slot field is provisioned automatically for Ethergroup.

Step 13 Click **Next**.

Step 14 Review the VLANs listed in the Available VLANs area. If the VLAN you want to use appears, continue with Step 16. If you need to create a new VLAN, complete the following steps:

a. Click the **New VLAN** button.

b. On the New VLAN dialog box, complete the following:

  - VLAN Name—Assign an easily-identifiable name to your VLAN.
  - VLAN ID—Assign a VLAN ID. The VLAN ID should be the next available number between 2 and 4093 that is not already assigned to an existing VLAN. Each ONS 15327 network supports a maximum of 509 user-provisionable VLANs.

c. Click **OK**.

Step 15 In the Available VLANs column, click the VLAN you want to use and click the arrow button (>>) to move the VLAN to the Circuit VLANs column.

Step 16 Click **Next**.

The Circuit Creation (Circuit Routing Preferences) dialog box opens.

Step 17 Verify the cross-connect information (in this step, "circuit" refers to the Ethernet cross-connect):

- Circuit name
- Circuit type
- Circuit size

- VLANs
- ONS 15327 nodes

If the information is not correct, click the **Back** button and repeat the procedure with the correct information.

Step 18 Click **Finish**.

Step 19 Complete the "DLP-B220 Provision E-Series Ethernet Ports" task on page 5-64.

Step 20 Complete the "DLP-B221 Provision E-Series Ethernet Ports for VLAN Membership" task on page 5-65.

Step 21 From the View menu choose **Go to Home View**.

Step 22 Click the **Circuits** tab.

Step 23 Highlight the circuit and click **Edit**.

The Edit Circuit dialog box opens.

Step 24 Click **Drops** and click **Create**.

The Define New Drop dialog box opens.

Step 25 From the **Slot** menu choose the OC-N card that links the ONS 15327 to the non-ONS 15327 equipment.

Step 26 From the **Port** menu choose the appropriate port.

Step 27 From the STS menu choose the STS that matches the STS of the connecting non-ONS equipment.

Step 28 Click **OK**.

Step 29 Confirm the circuit information that displays in the Edit Circuit dialog box and click **Close**.

Step 30 Repeat Steps 2 through 29 at the second Ethernet manual cross-connect endpoint.

The first and second Ethernet manual cross-connects will be bridged by the OC-N STS.

Note The appropriate STS circuit must exist in the non-ONS equipment to connect the two Ethernet manual cross-connect endpoints.

Caution If a CARLOSS alarm repeatedly appears and clears on an Ethernet manual cross-connect, the two Ethernet circuits might have a circuit-size mismatch. For example, a circuit size of STS-3c was configured on the first ONS 15327 and circuit size of STS-1 was configured on the second ONS 15327. Refer to the *Cisco ONS 15327 Troubleshooting Guide* if the alarm persists.

Step 31 Complete the "NTP-B146 Test E-Series Circuits" task on page 5-67.

Stop. You have completed this procedure.

DLP-B99 Determine Available VLANs

Purpose	This task verifies that the network has the capacity to support the additional new VLANs required for the creation E-Series circuits. It does not apply to E-Series cards in port-mapped mode.
Tools/Equipment	E-Series Ethernet cards must be installed at each end of the Ethernet circuit.
Prerequisite Procedures	NTP-B127 Verify Network Turn Up, page 5-3 DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 At any CTC view, click the **Circuits** tab.

Step 2 Click any existing Ethernet circuit to highlight that row.

Step 3 Click **Edit**, then click the **VLANs** tab.

The Edit Circuit dialog displays the number of VLANs used by circuits and the total number of VLANs available for use.

Step 4 Determine that number of available VLANs listed is sufficient for the number of E-series Ethernet circuits that you will create.

Caution Multiple E-series Ethernet circuits with spanning tree enabled will block each other if the circuits traverse the same E-series Ethernet card and use the same VLAN.

Step 5 Return to your originating procedure (NTP).

DLP-B246 Provision E-Series Ethernet Card Mode

Purpose	This task provisions an E-Series Ethernet card for multicard EtherSwitch Group, single-card EtherSwitch, or port-mapped mode.
Tools/Equipment	E-Series Ethernet cards must be installed.
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution You cannot change the mode while the Ethernet card is carrying circuits. If you want change the card mode, delete any circuits that it carries first. See the "NTP-B152 Delete Circuits" procedure on page 8-13.

Step 1 In the network view, double-click the node containing the E-Series Ethernet card you want to provision, then double-click the Ethernet card.

Step 2 Click the **Provisioning > Ether Card** tabs.

Step 3 In the Card Mode area, choose one of the following:

- For multicard EtherSwitch circuit groups, choose **Multicard EtherSwitch Group**. Click **Apply**.
- For single-card EtherSwitch circuits, choose **Single-card EtherSwitch**. Click **Apply**.
- For port-mapped circuits, choose **port-mapped**. Click **Apply**.

Step 4 Multicard EtherSwitch circuits only: repeat Steps 2 and 3 for all other Ethernet cards in the node that will carry the multicard EtherSwitch circuits.

Step 5 Repeat Steps this task for other nodes as necessary.

Step 6 Return to your originating procedure (NTP).

DLP-B220 Provision E-Series Ethernet Ports

Purpose	This task enables ports for the E-Series card.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security	Provisioning or higher

Step 1 Display the node view.

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

Step 3 Click the **Provisioning** > **Ether Port** tabs.

Step 4 For each Ethernet port, provision the following parameters:

- Port Name—If you want to label the port, type a port name.
- Mode—Choose the appropriate mode for the Ethernet port: Valid choices for the E-Series card are Auto, 10 Half, 10 Full, 100 Half, or 100 Full.
- Enabled—Check this check box to activate the corresponding Ethernet port.
- Priority—Choose a queuing priority for the port. Options range from 0 (Low) to 7 (High). Priority queuing (IEEE 802.1Q) reduces the impact of network congestion by mapping Ethernet traffic to different priority levels. Refer to the priority queuing information in the *Cisco ONS 15327 Reference Manual*. This parameter does not apply to an E-Series card in port-mapped mode.
- Stp Enabled—Check this check box to enable the spanning tree protocol (STP) on the port. This parameter does not apply to an E-Series card in port-mapped mode. Refer to the spanning tree information in the *Cisco ONS 15327 Reference Manual*.

Step 5 Click **Apply**.

Step 6 Repeat Steps 1 through 5 for all other cards in the VLAN or in port-mapped mode, the other card in a point-to-point circuit.

Step 7 The Ethernet ports are provisioned and ready to be configured for VLAN membership. See the "DLP-B221 Provision E-Series Ethernet Ports for VLAN Membership" task on page 5-65 for instructions.

Step 8 Return to your originating procedure (NTP).

DLP-B221 Provision E-Series Ethernet Ports for VLAN Membership

Purpose	This task provisions E-Series card ports for VLAN membership. It does not apply to E-Series cards in port-mapped mode.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Display the node view.

Step 2 Double-click the E-Series card graphic to open the card.

Step 3 Click the **Provisioning** > **Ether VLAN** tabs.

Step 4 To put a port in a VLAN:

a. Click the port and choose either Tagged or Untag. Table 5-4 shows valid port settings.

Table 5-4 VLAN Settings

Setting	Description
--	A port marked with this symbol does not belong to the VLAN.
Untag	The ONS 15327 will tag ingress frames and strip tags from egress frames.
Tagged	The ONS 15327 will process ingress frames according to the VLAN ID; egress frames will not have their tags removed.

b. If a port is a member of only one VLAN, choose **Untag** from the Port column in the VLAN's row. Choose **--** for all the other VLAN rows in that Port column.

Note The VLAN with **Untag** selected can connect to the port, but other VLANs cannot access that port.

c. Choose **Tagged** at all VLAN rows that need to be trunked. Choose **Untag** VLAN rows that do not need to be trunked, for example, the default VLAN.

Note Each Ethernet port must attach to at least one untagged VLAN. A trunk port connects multiple VLANs to an external device, such as a switch, which also supports trunking. A trunk port must have tagging (802.1Q) enabled for all the VLANs that connect to that external device.

Step 5 After each port is in the appropriate VLAN, click **Apply**.

Note .If Tagged is chosen, the attached external Ethernet devices must recognize IEEE 802.1Q VLANs.

Step 6 Return to your originating procedure (NTP).

NTP-B146 Test E-Series Circuits

Purpose	This procedure tests circuits created on E-Series Ethernet cards provisioned for multicard EtherSwitch Group, single-card EtherSwitch or port-mapped mode.
Tools/Equipment	Ethernet test set and appropriate fibers
Prerequisite Procedures	This procedure assumes that you completed facility loopback tests to test the fibers and cables from the source and destination ONS 15327s to the fiber distribution panel or the DSX, and one of the following: NTP-B191 Create an E-Series EtherSwitch Circuit (Multicard or Single-Card Mode), page 5-48 NTP-B142 Create an E-Series Shared Packet Ring Ethernet Circuit, page 5-52 NTP-B143 Create an E-Series Hub and Spoke Ethernet Configuration, page 5-55
Required/As Needed	As needed
Onsite/Remote	Onsite
Security	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at the ONS 15327 source node. If you are already logged in, continue with Step 2.

Step 2 On the shelf graphic, double-click the circuit source card.

Step 3 Click the **Provisioning > Ether Port** tabs.

Step 4 Verify the following settings:

- Mode— Auto, 10 Half, 10 Full, 100 Half, or 100 Full.
- Enabled—Checked.
- Priority—Set to the priority level indicated by the circuit or site plan. Priority does not apply to E-Series cards in port-mapped mode.
- Stp—Checked if Spanning Tree Protocol is enabled for the circuit. STP does not apply to E-Series cards in port-mapped mode.

Step 5 Click the **Ether VLAN** tab. If the E-Series cards is not in port-mapped mode, verify that the source port is on the same VLAN as the destination port.

Step 6 Repeat Steps 1 through 5 for the destination node.

Step 7 At the destination node, connect the Ethernet test set to the destination port and configure the test set to send and receive the appropriate Ethernet traffic.

Note At this point, you will not be able to send and receive Ethernet traffic.

Step 8 At the source node, connect an Ethernet test set to the source port and configure the test set to send and receive the appropriate Ethernet traffic.

Step 9 Transmit Ethernet frames between both test sets. If you cannot transmit and receive Ethernet traffic between the nodes, repeat Steps 1 through 8 to make sure you configured the Ethernet ports and test set correctly.

Step 10 Perform the protection switch testing appropriate to your SONET topology:

- For UPSRs, see the "DLP-B94 UPSR Protection Switching Test" task on page 4-25
- For BLSRs see the "DLP-B91 BLSR Ring Switch Test" task on page 4-19.

Configure your test set according to local site practice. For information about configuring your test set, see your test set user guide.

Step 11 After the Ethernet test is complete, print the results or save them to a disk for future reference. For information about printing or saving test results see your test set user guide.

Stop. You have completed this procedure.

NTP-B147 Create a G-Series Circuit

Purpose	This procedure creates a G-Series circuit.
Tools/Equipment	A G-Series Ethernet card must be installed at each end of the circuit.
Prerequisite Procedures	NTP-B127 Verify Network Turn Up, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at a node on the network where you will create the circuit. If you are already logged in, continue with Step 2.

Step 2 From the View menu choose **Go to Network View**.

Step 3 Click the **Circuits** tab and click **Create**.

Step 4 In the Create Circuits dialog box, complete the following fields:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Type—Choose STS.
- Size—Choose the circuit size. Valid circuit sizes for a G-Series circuit are STS-1, STS-3c, STS6c, STS-9c, STS-12c, STS-24c, and STS-48c.
- Bidirectional—Leave the default unchanged (checked).
- Number of circuits—Leave the default unchanged (1).
- State—Choose a service state to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS— The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).

- OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and permits loopbacks on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-B230 Change a Circuit State" task on page 8-7.

- Apply to drop ports—Check this check box if you want to apply the state chosen in the State field (IS or OOS-MT only) to the Ethernet circuit source and destination ports. You cannot apply OOS-AINS to G-Series Ethernet card ports. CTC will apply the circuit state to the ports only if the circuit bandwidth is the same as the port bandwidth or, if the port bandwidth is larger than the circuit, the circuit must be the first circuit to use the drop port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If the check box is unchecked, CTC will not change the state of the source and destination ports.

Note LOS alarms appear if in service (IS) ports are not receiving signals.

- Create cross-connects only (TL1-like)—Uncheck this check box.
- Inter-domain (UCP) SLA—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Auto-ranged—Unavailable.
- Protected Drops—Leave the default unchanged (unchecked).

Step 5 If the circuit will be routed on a UPSR, complete the "DLP-B218 Provision UPSR Selectors During Circuit Creation" task on page 5-25.

Step 6 Click **Next**.

Step 7 Provision the circuit source:

a. From the Node drop-down menu choose the circuit source node. Either end node can be the point-to-point circuit source.

b. From the Slot drop-down menu choose the slot containing the G-Series card that you will use for one end of the point-to-point circuit.

c. From the Port drop-down menu choose a port.

Step 8 Click **Next**.

Step 9 Provision the circuit destination:

a. From the Node drop-down menu choose the circuit destination node.

b. From the Slot drop-down menu choose the slot containing the G-Series card that you will use for other end of the point-to-point circuit.

c. From the Port drop-down menu choose a port.

Step 10 Click **Next**. The Circuits window appears.

Step 11 Confirm that the following circuit information is correct:

- Circuit name
- Circuit type
- Circuit size
- ONS 15327 circuit nodes

Step 12 Click **Finish**.

Note To change the capacity of a G-Series circuit, you must delete the original circuit and reprovision a new larger circuit.

Step 13 Complete the "NTP-B149 Test G-Series Circuits" procedure on page 5-73.

Stop. You have completed this procedure.

NTP-B148 Create a Manual Cross-Connect for a G-Series or an E-Series in Port-Mapped Mode

Purpose	This procedure creates a manual cross-connect between a G-Series Ethernet card or an E-Series card in port-mapped mode and an OC-N card connected to non-ONS equipment.
Tools/Equipment	A G-Series or E-Series card must be installed at the circuit source node.
Prerequisite Procedures	NTP-B127 Verify Network Turn Up, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note In this procedure, cross-connect refers to a circuit connection created within the same node between the Ethernet card and an OC-N card connected to third-party equipment. You create cross-connects at the source and destination nodes so an Ethernet circuit can be routed from source to destination across third-party equipment.

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at a node where you will create the cross-connect. If you are already logged in, continue with Step 2.

Step 2 If you are provisioning an E-Series card, verify that the Ethernet card that will carry the circuit is provisioned for port-mapped mode. See the "DLP-B246 Provision E-Series Ethernet Card Mode" task on page 5-64.

Step 3 Click the **Circuits** tab and click **Create**.

Step 4 In the Create Circuits dialog box, complete the following fields:

- Name—Assign a name to the source cross-connect. The name can be alphanumeric and up to 48 characters (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the source cross-connect.
- Type—Choose STS.
- Size—Choose the size of the circuit that will be carried by the cross-connect. Valid sizes for a G-Series circuit are STS-1, STS-3c, STS-6c, STS-9c, STS-12c, STS-24c, and STS-48c. For an E-Series in port-mapped mode, valid sizes are STS-1, STS-3c, STS-6c, and STS-12c.
- Bidirectional—Leave the default unchanged (checked).
- Number of circuits—Leave the default unchanged (1).

- Auto-ranged—Unavailable.
- State—Choose a service state to apply to the circuit after it is created:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit.
  - OOS-AINS—The circuit is out of service until it receives a valid signal, at which time the circuit state automatically changes to in service (IS).
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and permits loopbacks on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete. See the "DLP-B230 Change a Circuit State" task on page 8-7.
- Apply to drop ports—Uncheck this check box.
- Create cross-connects only (TL1-like)—Uncheck this check box
- Inter-domain (UCP) SLA—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Leave the default unchanged (unchecked).

Step 5 If the circuit will be routed on a UPSR, complete the "DLP-B218 Provision UPSR Selectors During Circuit Creation" task on page 5-25.

Step 6 Click **Next**.

Step 7 Provision the circuit source:

a. From the Node drop-down menu choose the circuit source node.

b. From the Slot drop-down menu choose the Ethernet card that will be the cross-connect source.

c. From the Port drop-down menu choose the cross-connect source port.

Step 8 Click **Next**.

Step 9 Provision the circuit destination:

a. From the Node drop-down menu choose the same node selected as the circuit source. For Ethernet cross-connects, the source and destination nodes are the same.

b. From the Slot drop-down menu choose the OC-N card that connects to the non-ONS equipment.

c. Depending on the OC-N card, choose the port and STS from the Port and STS drop-down menus.

Step 10 Click **Next**.

Step 11 Verify the cross-connect information (in this step, "circuit" refers to the cross-connect):

- Circuit name
- Circuit type
- Circuit size
- ONS 15327 circuit nodes

If the information is not correct, click the **Back** button and repeat the procedure with the correct information.

Step 12 Click **Finish**.

Step 13 Complete the "NTP-B149 Test G-Series Circuits" procedure on page 5-73 for the G-Series circuit, or complete the "NTP-B146 Test E-Series Circuits" procedure on page 5-67 for the E-Series in port-mapped mode circuit.

Stop. You have completed this procedure.

DLP-B222 Provision G-Series Ethernet Ports

Purpose	This task provisions G-Series Ethernet ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	Required to enable Ethernet traffic on the G-Series
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, double-click the G-Series card graphic to open the card.

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

Step 3 For each G-Series port, provision the following parameters:

- Port Name—If you want to label the port, type the port name.
- State—Choose **IS** to put the port in service.
- Flow Control Neg—Click this check box to enable flow control negotiation on the port. If you do not want to enable flow control, uncheck the box.

Note To activate flow control, the Ethernet device attached to the G-Series card must be set to auto-negotiation. If flow control is enabled but the negotiation status indicates no flow control, check the auto-negotiation settings on the attached Ethernet device.

- Max Size—To permit the acceptance of jumbo size Ethernet frames, choose **Jumbo**. If you do not want to permit jumbo size Ethernet frames, choose **1548**.

Note The maximum frame size of 1548 bytes enables the port to accept valid Ethernet frames that use protocols, such as Inter-Switch Link (ISL). ISL adds 30 bytes of overhead and may cause the frame size to exceed the traditional 1518 byte maximum.

Step 4 Click **Apply**.

Step 5 Refresh the Ethernet statistics:

a. Click the **Performance > Statistics** tabs.

b. Click the **Refresh** button.

Note Reprovisioning an Ethernet port on the G-Series card does not reset the Ethernet statistics for that port.

Step 6 Return to your originating procedure (NTP).

NTP-B149 Test G-Series Circuits

Purpose	This procedure tests circuits created on G-Series Ethernet cards.
Tools/Equipment	Ethernet test set and appropriate fibers
Prerequisite Procedures	This procedure assumes that you completed facility loopback tests to test the fibers and cables from the source and destination ONS 15327s to the fiber distribution panel or the DSX. NTP-B147 Create a G-Series Circuit, page 5-68 or NTP-B148 Create a Manual Cross-Connect for a G-Series or an E-Series in Port-Mapped Mode, page 5-70
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at the ONS 15327 source node. If you are already logged in, continue with Step 2.

Step 2 Change the circuit and circuit ports to an OOS-MT service state:

a. Click the **Circuits** tab.

b. Click the circuit you want to test.

c. From the Tools menu choose **Circuits > Change Circuit State**.

d. On the Change Circuit State dialog box, choose **OOS_MT** from the Target Circuit State drop-down menu.

e. Check the **Apply to circuit drops** check box.

f. Click **OK**.

Step 3 On the shelf graphic, double-click the circuit source card.

Step 4 Click the **Provisioning > Port** tabs.

Step 5 Verify the following settings:

- State—OOS_MT
- Flow Control Neg—Checked or unchecked as indicated by the circuit or site plan
- Max Size—Check or unchecked as indicated by the circuit or site plan
- Media Type—SX or LX

Step 6 Repeat Steps 1 through 5 for the destination node.

Step 7 At the destination node connect the Ethernet test to the destination port and configure the test set to send and receive the appropriate Ethernet traffic.

Note At this point, you will not be able to send and receive Ethernet traffic.

Step 8 At the source node connect an Ethernet test set to the source port and configure the test set to send and receive the appropriate Ethernet traffic.

Step 9 Transmit Ethernet frames between both test sets. If you cannot transmit and receive Ethernet traffic between the nodes, repeat Steps 1 through 6 to make sure you configured the Ethernet ports and test set correctly.

Step 10 Perform the protection switch that is appropriate to the SONET topology:

- For UPSRs, see the "DLP-B94 UPSR Protection Switching Test" task on page 4-25.
- For BLSRs see the "DLP-B91 BLSR Ring Switch Test" task on page 4-19.

Configure your test set according to local site practice. For information about configuring your test set, see your test set user guide.

Step 11 Change the circuit and circuit ports to the IS service state:

a. Click the **Circuits** tab.

b. Choose the circuit you want to test.

c. From the Tools menu choose **Circuits > Change Circuit State**.

d. In the Change Circuit State dialog box, choose **IS** from the Target Circuit State drop-down menu.

e. Check the **Apply to circuit drops** check box.

f. Click **OK**.

Step 12 After the circuit test is complete, print the results or save them to a disk for future reference. For information about printing or saving test results see your test set user guide.

Stop. You have completed this procedure.

NTP-B194 Create Overhead Circuits

Purpose	This procedure creates overhead circuits on an ONS 15327 network. Overhead circuits include DCC tunnels, orderwire, and user data channels.
Tools/Equipment	None
Prerequisite Procedures	NTP-B127 Verify Network Turn Up, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at a node on the network where you will create the overhead circuit. If you are already logged in, continue with Step 2.

Step 2 From the View menu choose **Go to Network View**.

Step 3 As needed, complete the "DLP-B313 Create a DCC Tunnel" task on page 5-75.

Step 4 As needed, complete the "DLP-B212 Create a User Data Channel" task on page 5-76.

Stop. You have completed this procedure.

DLP-B313 Create a DCC Tunnel

Purpose	This task creates a DCC tunnel to transport traffic from third-party SONET equipment across ONS 15327 networks. Tunnels can be created on the Section DCC channel (D1-D3) (if not used by the ONS 15327 as a terminated DCC), or any Line DCC channel (D4-D6, D7-D9, or D10-D12).
Tools/Equipment	None
Prerequisite Procedures	NTP-B127 Verify Network Turn Up, page 5-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Each ONS 15327 can have up to 32 DCC tunnel connections. Terminated Section DCCs used by the ONS 15327 cannot be used as DCC tunnel endpoints, and a Section DCC that is used as an DCC tunnel endpoint cannot be terminated. All DCC tunnel connections are bidirectional.

Step 1 In network view, click the **Provisioning > Overhead Circuits** tabs.

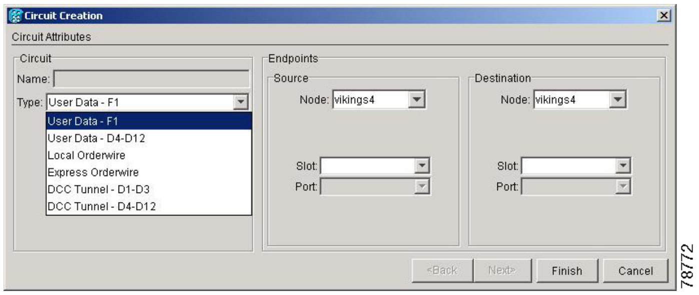
Step 2 Click **Create**.

Step 3 In the Circuit Creation dialog box (Figure 5-12), provision the DCC tunnel:

- Name—Type the tunnel name.
- Type—Choose one:
  - DCC Tunnel-D1-D3—Allows you to choose either the Section DCC (D1-D3) or a Line DCC (D4-D6, D7-D9, or D10-D12) as the source or destination endpoints.
  - DCC Tunnel-D4-D12—Provisions the full Line DCC as a tunnel.
- Source Node—Choose the source node.
- Slot—Choose the source slot.
- Port—If displayed, select the source port.
- Channel—Displayed if you chose DCC Tunnel-D1-D3 as the tunnel type. Choose one of the following:
  - DCC1 (D1-D3)—Section DCC
  - DCC2 (D4-D6)—Line DCC 1
  - DCC3 (D7-D9)—Line DCC 2
  - DCC4 (D10-D12)—Line DCC 3

  DCC options are not displayed if they are used by the ONS 15327 (DCC1) or other tunnels.

Figure 5-12 Provisioning a DCC Tunnel



Type: User Data - F1

Source Node: vikings4

Destination Node: vikings4

Step 4 Click **OK**.

Step 5 Put the ports that are hosting the DCC tunnel in service. See the "DLP-B214 Change the Service State for a Port" task on page 4-5 for instructions.

Step 6 Return to your originating procedure (NTP).

DLP-B212 Create a User Data Channel

Purpose	This task creates a user data channel (UDC) on the ONS 15327. A UDC circuit allows you to create a dedicated data channel between nodes.
Tools/Equipment	None
Prerequisite Procedures	NTP-B24 Verify Card Installation, page 3-2 DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In network view, click the **Provisioning > Overhead Circuits** tabs.

Step 2 Click **Create**.

Step 3 In the Circuit Creation dialog box, complete the following fields:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces).
- Type—Choose either User Data-F1 or User Data D-4-D-12 from the drop-down menu.

Step 4 In the Endpoints area, choose the source and destination nodes and the source and destination optical ports and slots from the drop-down menus.

Step 5 Click **Finish**.

Step 6 Return to your originating procedure (NTP).

Manage Alarms

This chapter explains how to view and manage the alarms and conditions on a Cisco ONS 15327.

Cisco Transport Controller (CTC) detects and reports SONET alarms generated by the Cisco ONS 15327 and the larger SONET network. You can use CTC to monitor and manage alarms at a card, node, or network level. You can also view alarm counts on the LCD front panel.

Before You Begin

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-B195 Document Existing Provisioning, page 6-2—Complete this procedure as needed to record node information or to troubleshoot rings and spans.
2. NTP-B196 View Alarms, History, Events, and Conditions, page 6-5—Complete this procedure as needed to see alarms and conditions occurring on the node and a complete history of alarm and condition messages.
3. NTP-B68 Delete Cleared Alarms from Display, page 6-12—Complete this procedure as needed to delete cleared alarm information that is no longer needed.
4. NTP-B69 View Alarm-Affected Circuits, page 6-13—Complete this procedure as needed to find circuits that are affected by a particular alarm or condition.
5. NTP-B70 Create, Download, and Assign Alarm Severity Profiles, page 6-15—Complete this procedure as needed to change the default severity for certain alarms, assign the new severities to a port, card, or node, and delete alarm profiles.
6. NTP-B168 Enable, Modify, or Disable Alarm Severity Filtering, page 6-25—Complete this procedure as needed to enable, disable, or modify alarm severity filtering in the Conditions, Alarms, or History screens; you can enable, modify, and disable alarm severity filtering at the node or network level.
7. NTP-B72 Suppress and Discontinue Alarm Suppression, page 6-29—As needed, use these tasks to suppress reported alarms at the port, card, or node level and disable the suppress command to resume normal alarm reporting.

NTP-B195 Document Existing Provisioning

Purpose	Use this procedure to print card, node, or network CTC information in graphical or tabular form on a Windows-provisioned printer, or to export card, node, or network information as editable delineated text files to other applications. This procedure is useful for network record keeping and troubleshooting.
Tools/Equipment	Printer connected to the CTC computer by a direct or network connection
Prerequisite Procedures	Chapter 3, "Turn Up Node"
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at the node that has the information you want to record or save. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "DLP-B138 Print CTC Data" task on page 6-2.

Step 3 As needed, complete the "DLP-B139 Export CTC Data" task on page 6-3.

Stop. You have completed this procedure.

DLP-B138 Print CTC Data

Purpose	Use this task to print CTC card, node, or network data in graphical or tabular form on a Windows-provisioned printer.
Tools/Equipment	Printer connected to the CTC computer by a direct or network connection
Prerequisite procedures	DLP-B60 Log into CTC, page 2-23
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Click the CTC tab (and subtab, if present) containing the information you want to print. For example, click the **Alarms** tab to print Alarms window data.

The print operation is available for all network, node (default login), and card view windows.

Step 2 From the File menu, choose **Print**.

Step 3 In the Print dialog box, click a a printing option (Figure 6-1).

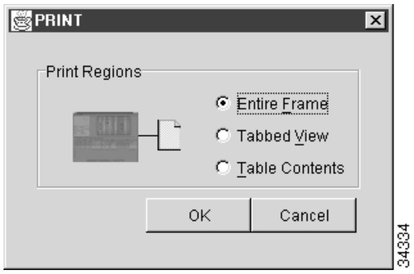
- Entire Frame—Prints the entire CTC window including the graphical view of the card, node, or network. This option is available for all windows.
- Tabbed View—Prints the lower half of the CTC window containing tabs and data. The printout includes the selected tab (on top) and the data shown in the tab window. For example, if you print the History window Tabbed View, you print only history items appearing in the window. This option is available for all windows.

- Table Contents—Prints CTC data in table format without graphical representations of shelves, cards, or tabs. This option is available only for CTC table data, so it does not apply to:
  - Provisioning > General, Protection, Security, SNMP, SONET DCC, or Timing windows
  - Maintenance > Database, Protection, Diagnostic, or Timing windows

  The Table Contents option prints all the data contained in a table with the same column headings. For example, if you print the History window Table Contents view, you print all data included in the table whether or not items appear in the window.

Tip When you print using the Tabbed View option, it can be difficult to distinguish whether the printout applies to the network, node, or card view. Look at the tabs to determine which view you are printing. Network, node, and card views are identical except that network view does not contain an Inventory tab; node view and card view contain a Performance tab.

Figure 6-1 Selecting CTC Data For Print


PRINT

Print Regions

● Entire Frame
○ Tabbed View
○ Table Contents

Step 4 Click **OK**.

Step 5 In the Windows Print dialog box, click a printer and click **OK**.

Step 6 Repeat this task for each window that you want to print.

Step 7 Return to your originating procedure (NTP).

DLP-B139 Export CTC Data

Purpose	Use this task to export CTC table data as delineated text to view or edit the data in text editor, word processing, spreadsheet, database management, or web browser applications.
Tools/Equipment	None
Prerequisite procedures	DLP-B60 Log into CTC, page 2-23
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Click the CTC tab containing the information you want to export (for example, the Alarms tab or the Circuits tab).

Step 2 From the File menu choose **Export**.

Step 3 In the Export dialog box (Figure 6-2), click a data format:

- As HTML—Saves data as a simple HTML table file without graphics. The file must be viewed or edited with applications such as Netscape Navigator, Microsoft Internet Explorer, or other applications capable of opening HTML files.
- As CSV—Saves the CTC table as comma-separated values (CSV).
- As TSV—Saves the CTC table as tab-separated values (TSV).

Step 4 If you want to open a file in a text editor or word processor application, procedures may vary; typically you can use the File > Open command to display the CTC data, or you can double-click the file name and choose an application such as Notepad.

Text editor and word processor applications display the data exactly as it is exported, including comma or tab separators. All applications that open the data files allow you to format the data.

Step 5 If you want to open the file in spreadsheet and database management applications, procedures may vary; typically you need to open the application and choose File > Import, then choose a delimited file to display the data in cells.

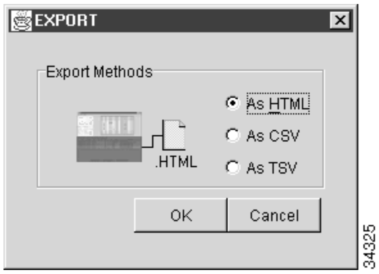
Spreadsheet and database management programs also allow you to manage the exported data.

Note An exported file cannot be opened in CTC.

The export operation only applies to tabular data, so it is not available for the following CTC tabs and subtabs:

- Provisioning > General, Protection, Security, SNMP, SONET DCC, or Timing windows
- Maintenance > Database, Protection, Diagnostic, or Timing windows

Figure 6-2 Selecting CTC Data For Export



EXPORT

Export Methods

● As HTML
○ As CSV
○ As TSV

Step 6 Click **OK**.

Step 7 In the Save dialog box, enter a name in the File name field using one of the following formats:

- [filename].html—for HTML files
- [filename].csv—for CSV files
- [filename].tsv—for TSV files

Step 8 Navigate to a directory where you want to store the file.

Step 9 Click **OK**.

Step 10 Repeat the task for each window that you want to export.

Step 11 Return to your originating procedure (NTP).

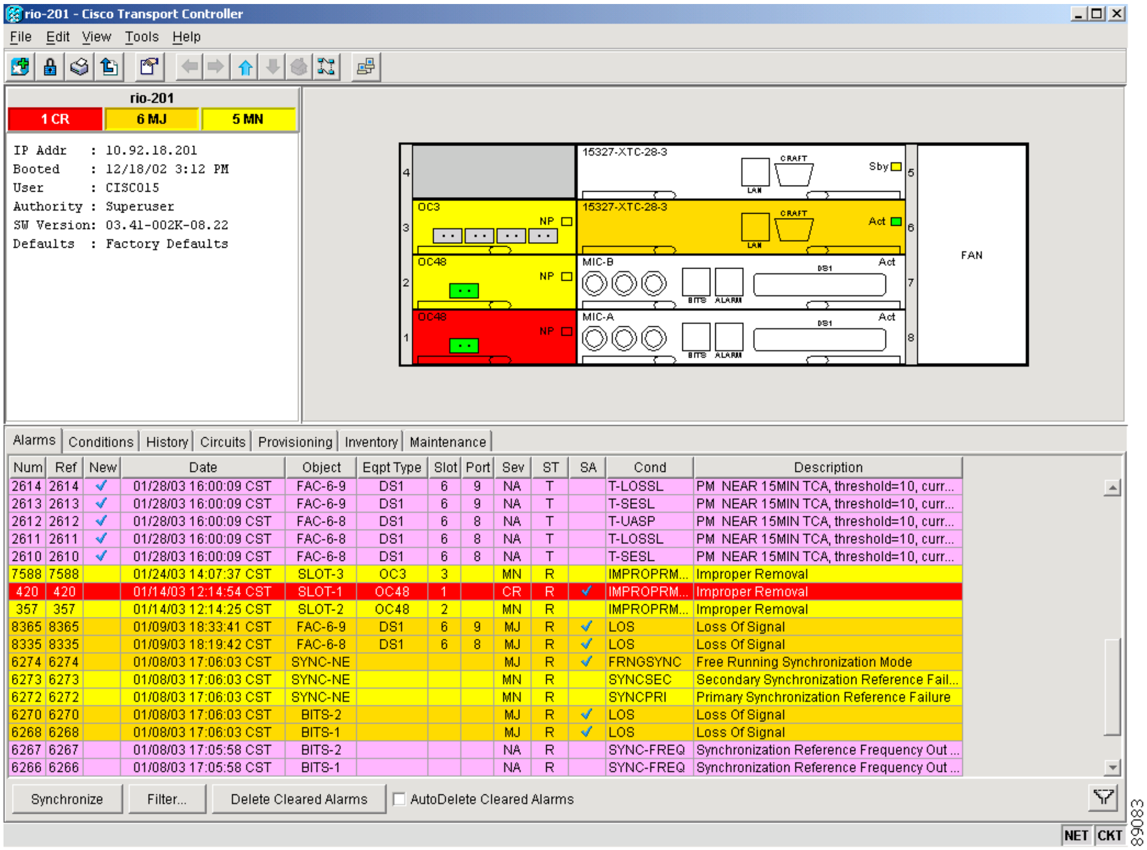
NTP-B196 View Alarms, History, Events, and Conditions

Purpose	Use this procedure to view current or historical alarms and conditions for a card, a node, or network. This information is useful for monitoring and troubleshooting hardware and software events.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning

Step 1 Log into the node that contains the alarms you want to view. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. If you are already logged in, proceed to Step 2.

Step 2 In the card, node (default), or network-level CTC view, click the **Alarms** tab to display the alarms for that card, node, or network (Figure 6-3 on page 6-6).

Figure 6-3 ONS 15327 CTC Node (Login) View



```
IP Addr   : 10.92.18.201
Booted    : 12/18/02 3:12 PM
User      : CISCO15
Authority : Superuser
SW Version: 03.41-002K-08.22
Defaults  : Factory Defaults
```

Alarms | Conditions | History | Circuits | Provisioning | Inventory | Maintenance

Num	Ref	New	Date	Object	Eqpt Type	Slot	Port	Sev	ST	SA	Cond	Description
2614	2614	✓	01/28/03 16:00:09 CST	FAC-6-9	DS1	6	9	NA	T		T-LOSSL	PM NEAR 15MIN TCA, threshold=10, curr...
2613	2613	✓	01/28/03 16:00:09 CST	FAC-6-9	DS1	6	9	NA	T		T-SESL	PM NEAR 15MIN TCA, threshold=10, curr...
2612	2612	✓	01/28/03 16:00:09 CST	FAC-6-8	DS1	6	8	NA	T		T-UASP	PM NEAR 15MIN TCA, threshold=10, curr...
2611	2611	✓	01/28/03 16:00:09 CST	FAC-6-8	DS1	6	8	NA	T		T-LOSSL	PM NEAR 15MIN TCA, threshold=10, curr...
2610	2610	✓	01/28/03 16:00:09 CST	FAC-6-8	DS1	6	8	NA	T		T-SESL	PM NEAR 15MIN TCA, threshold=10, curr...
7588	7588		01/24/03 14:07:37 CST	SLOT-3	OC3	3		MN	R		IMPROPRM...	Improper Removal
420	420		01/14/03 12:14:54 CST	SLOT-1	OC48	1		CR	R	✓	IMPROPRM...	Improper Removal
357	357		01/14/03 12:14:25 CST	SLOT-2	OC48	2		MN	R		IMPROPRM...	Improper Removal
8365	8365		01/09/03 18:33:41 CST	FAC-6-9	DS1	6	9	MJ	R	✓	LOS	Loss Of Signal
8335	8335		01/09/03 18:19:42 CST	FAC-6-8	DS1	6	8	MJ	R	✓	LOS	Loss Of Signal
6274	6274		01/08/03 17:06:03 CST	SYNC-NE				MJ	R	✓	FRNGSYNC	Free Running Synchronization Mode
6273	6273		01/08/03 17:06:03 CST	SYNC-NE				MN	R		SYNCSEC	Secondary Synchronization Reference Fail...
6272	6272		01/08/03 17:06:03 CST	SYNC-NE				MN	R		SYNCPRI	Primary Synchronization Reference Failure
6270	6270		01/08/03 17:06:03 CST	BITS-2				MJ	R	✓	LOS	Loss Of Signal
6268	6268		01/08/03 17:06:03 CST	BITS-1				MJ	R	✓	LOS	Loss Of Signal
6267	6267		01/08/03 17:05:58 CST	BITS-2				NA	R		SYNC-FREQ	Synchronization Reference Frequency Out ...
6266	6266		01/08/03 17:05:58 CST	BITS-1				NA	R		SYNC-FREQ	Synchronization Reference Frequency Out ...

Synchronize | Filter... | Delete Cleared Alarms | □ AutoDelete Cleared Alarms

Table 6-1 lists the columns in the Alarms window and their descriptions.

Table 6-1 Alarm Column Descriptions

Column	Information Recorded
New	Indicates a new alarm; to change this status, click either the Synchronize button or the Delete Cleared Alarms button
Date	Date and time of the alarm
Node	Node where the alarm occurred (appears only in network view)
Object	TL1 access identifier (AID) for the alarmed object. For an STSmon or VTmon, this is the monitored STS or VT object.
Eqpt Type	Card type in this slot
Slot	Slot where the alarm occurred (appears only in network and node view)
Port	Port where the alarm is raised. For STSTerm and VTTerm, the port refers to the upstream card it is partnered with.
Sev	Severity level: CR (critical), MJ (major), MN (minor), NA (not-alarmed), NR (not-reported)
ST	Status: R (raised), C (clear)
SA	When selected (checked), indicates a service-affecting alarm

Table 6-1 Alarm Column Descriptions (continued)

Column	Information Recorded
Cond	The error message/alarm name; these names are alphabetically defined in the "Alarm Troubleshooting" chapter of the *Cisco ONS 15327 Troubleshooting Guide*
Description	Description of the alarm
Num	A count of incrementing alarm messages
Ref	The reference number assigned to the alarm

Table 6-2 lists the color codes for alarm and condition severities.

Table 6-2 Color Codes for Alarms and Conditions

Color	Description
Red	Raised Critical (CR) alarm
Orange	Raised Major (MJ) alarm
Yellow	Raised Minor (MN) alarm
Magenta (pink)	Raised Not-Alarmed (NA) condition
Blue	Raised Not-Reported (NR) condition
White	Cleared (C) alarm or condition

Step 3 If alarms are present, refer to the *Cisco ONS 15327 Troubleshooting Guide* for information and troubleshooting procedures.

Step 4 Complete the "DLP-B110 View Alarm History" task on page 6-7, the "DLP-B113 Synchronize Alarms" task on page 6-10, or the "DLP-B114 View Conditions" task on page 6-11 as needed.

Stop. You have completed this procedure.

DLP-B110 View Alarm History

Purpose	Use this task to view past cleared and uncleared ONS 15327 alarm messages at the card, node, or network level. This task is useful for troubleshooting configuration, traffic, or connectivity issues that are indicated by alarms.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 To view node alarm history, proceed to Step 2. To view network alarm history, proceed to Step 3. To view card alarm history, proceed to Step 5.

Step 2 To view node alarm history:

- **a.** Click the **History > Session** tabs if you want to view the alarms and conditions (events) raised during the current session (since you logged into the CTC).
- **b.** Click the **History > Node** tabs to retrieve all available alarm messages for the node.

Tip Double-click an alarm in the alarm table or an event (condition) message in the history table to display the view that corresponds to the alarm message. Double-click a card alarm to display the card view. In network view, double-click a node alarm to display the node view.

Step 3 To view network alarm history, from node view click **View > Go to Network View**.

Step 4 Click the **History** tab.

Alarms and conditions (events) raised during the current session appear.

Step 5 To view card alarm history, from the network view click **View > Go to Previous View**.

The previous view is the node (default login) view.

Step 6 From node view, double-click a card on the shelf graphic to display the card-level view for the card.

Note Mechanical Interface cards (MICs) do not have a card view.

- **a.** Click the **History > Session** tabs to view the alarm messages raised during the current session.
- **b.** Click the **History > Card** tabs to retrieve all available alarm messages for the card.

Note The ONS 15327 can store up to 640 critical alarm messages, 640 major alarm messages, 640 minor alarm messages, and 640 condition messages. When any of these limits is reached, the ONS 15327 discards the oldest events in that category.

Step 7 In the node or card view, display Not-Alarmed (NA) and transient event (condition) history in addition to alarm history by clicking the **Events** check box in the History > Node window or History > Card window.

Step 8 Click **Retrieve**.

Step 9 The window displays raised and cleared alarm messages (and events, if selected).

Tip Double-click an alarm in the alarm table or a condition in the history table to display the view that corresponds to the alarm message. 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.

Step 10 Return to your originating procedure (NTP).

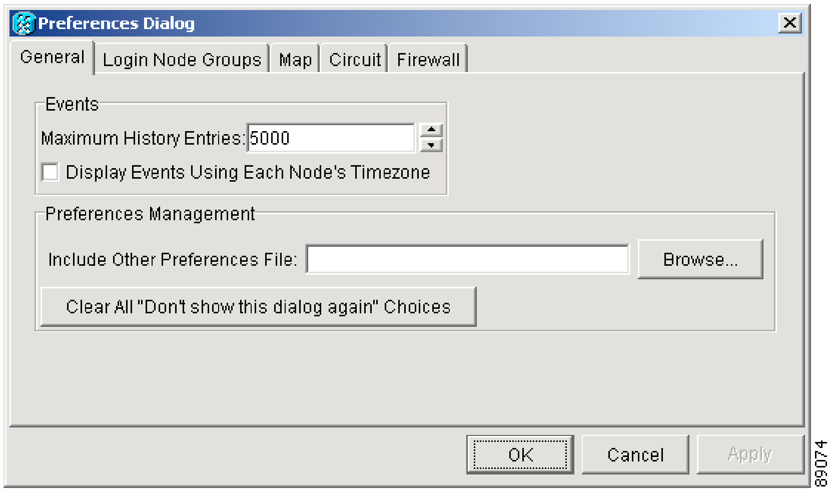
DLP-B111 Changing the Maximum Number of Session Entries for Alarm History

Purpose	This task changes the maximum number of session entries included in the alarm history. Use this task to extend the history list in order to save information for future reference or troubleshooting.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning

Step 1 From the Edit menu choose **Preferences**.

The CTC Preferences Dialog box appears (Figure 6-4).

Figure 6-4 CTC Preferences Dialog Box



Events
Maximum History Entries: 5000
□ Display Events Using Each Node's Timezone

Step 2 Click the up or down arrow buttons next to the Maximum History Entries field to change the entry.

Step 3 Click **Apply** and **OK**.

Note Setting the Maximum History Entries value to the high end of the range uses more CTC memory and could impair CTC performance.

Note This task changes the maximum history entries recorded for CTC sessions. It does not affect the maximum number of history entries viewable for a network, node, or card.

Step 4 Return to your originating procedure (NTP).

DLP-B112 Display Alarms and Conditions Using Time Zone

Purpose	Use this task to change the timestamp for events to the timezone of the ONS node reporting the alarm. By default, the events timestamp is set to the timezone for the CTC workstation.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning

Step 1 From the Edit menu choose **Preferences**.

The CTC Preferences Dialog box appears (Figure 6-4 on page 6-9).

Step 2 Click the **Display Events Using Each Node's Timezone** check box.

Step 3 Click **Apply** and **OK**.

Step 4 Return to your originating procedure (NTP).

DLP-B113 Synchronize Alarms

Purpose	Use this task to view ONS 15327 events at the card, node, or network level and to refresh the alarm listing while troubleshooting so that you can check for new and cleared alarms and conditions.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 At the card, node, or network view, click the **Alarms** tab.

Step 2 Click **Synchronize**.

This button causes CTC to retrieve a current alarm summary for the card, node, or network. This step is optional because CTC updates the Alarms window automatically as messages arrive from the node.

Alarms that have been raised during the session will have a check mark in the Alarms window New column. When you click Synchronize, the check mark disappears.

Step 3 Return to your originating procedure (NTP).

DLP-B114 View Conditions

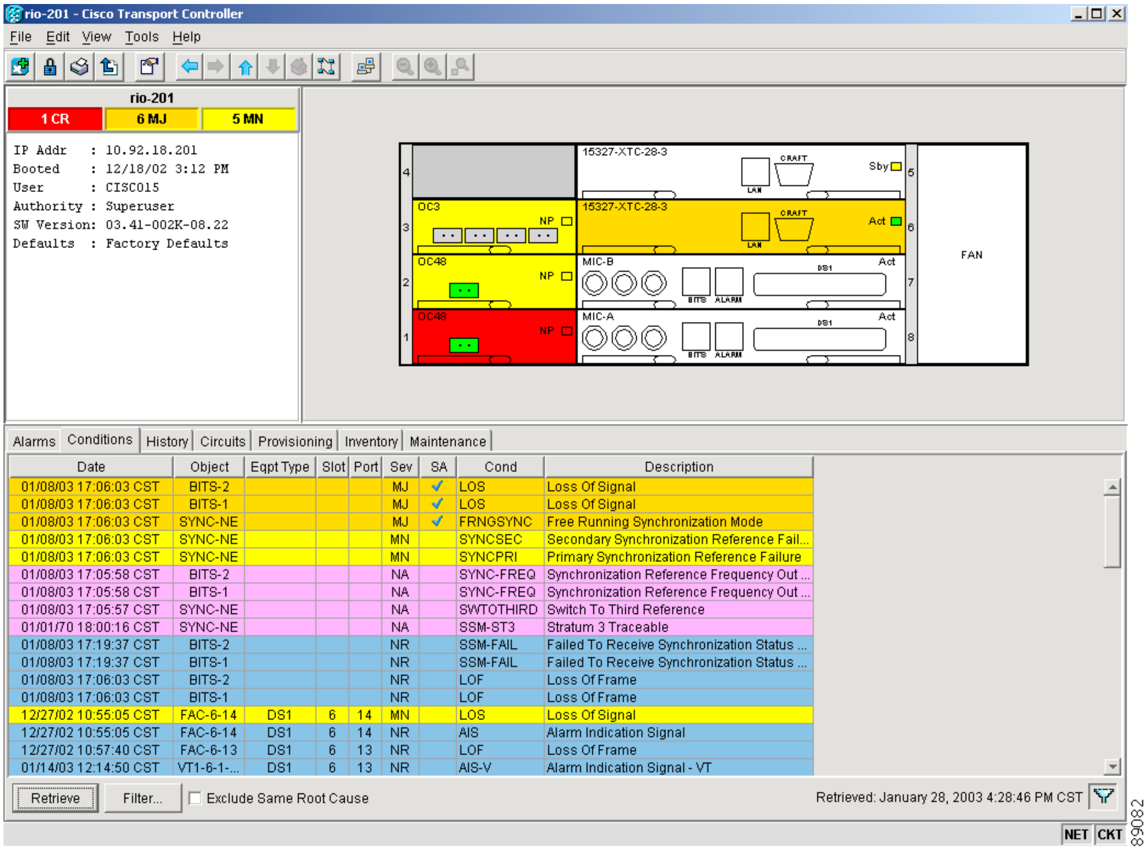
Purpose	Use this task to view conditions, [events with a Not-Reported (NR) severity] at the card, node, or network level. Conditions give you a clear record of changes or events that do not result in alarms.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 In the card, node, or network view, click the **Conditions** tab.

Step 2 Click **Retrieve** (Figure 6-5).

The Retrieve button requests the current set of fault conditions from the node, card, or network. The window is not updated when conditions change on the node. You must click Retrieve to see any changes.

Figure 6-5 Node View Conditions Window



```
IP Addr   : 10.92.18.201
Booted    : 12/18/02 3:12 PM
User      : CISCO15
Authority : Superuser
SW Version: 03.41-002K-08.22
Defaults  : Factory Defaults
```

Date	Object	Eqpt Type	Slot	Port	Sev	SA	Cond	Description
01/08/03 17:06:03 CST	BITS-2				MJ	✓	LOS	Loss Of Signal
01/08/03 17:06:03 CST	BITS-1				MJ	✓	LOS	Loss Of Signal
01/08/03 17:06:03 CST	SYNC-NE				MJ	✓	FRNGSYNC	Free Running Synchronization Mode
01/08/03 17:06:03 CST	SYNC-NE				MN		SYNCSEC	Secondary Synchronization Reference Fail...
01/08/03 17:06:03 CST	SYNC-NE				MN		SYNCPRI	Primary Synchronization Reference Failure
01/08/03 17:05:58 CST	BITS-2				NA		SYNC-FREQ	Synchronization Reference Frequency Out ...
01/08/03 17:05:58 CST	BITS-1				NA		SYNC-FREQ	Synchronization Reference Frequency Out ...
01/08/03 17:05:57 CST	SYNC-NE				NA		SWTOTHIRD	Switch To Third Reference
01/01/70 18:00:16 CST	SYNC-NE				NA		SSM-ST3	Stratum 3 Traceable
01/08/03 17:19:37 CST	BITS-2				NR		SSM-FAIL	Failed To Receive Synchronization Status ...
01/08/03 17:19:37 CST	BITS-1				NR		SSM-FAIL	Failed To Receive Synchronization Status ...
01/08/03 17:06:03 CST	BITS-2				NR		LOF	Loss Of Frame
01/08/03 17:06:03 CST	BITS-1				NR		LOF	Loss Of Frame
12/27/02 10:55:05 CST	FAC-6-14	DS1	6	14	MN		LOS	Loss Of Signal
12/27/02 10:55:05 CST	FAC-6-14	DS1	6	14	NR		AIS	Alarm Indication Signal
12/27/02 10:57:40 CST	FAC-6-13	DS1	6	13	NR		LOF	Loss Of Frame
01/14/03 12:14:50 CST	VT1-6-1-...	DS1	6	13	NR		AIS-V	Alarm Indication Signal - VT

☐ Exclude Same Root Cause

Retrieved: January 28, 2003 4:28:46 PM CST

Conditions include all fault conditions raised on the node, whether or not they are reported.

Note Alarms can be unreported when they are filtered out of the display. See the "DLP-B225 Enable Alarm Filtering" section on page 6-26 for information.

Events that are reported as Major (MJ), Minor (MN), or Critical (CR) severities are alarms. Events that are reported as Not-Alarmed (NA) are conditions. Conditions that are not reported at all are marked Not-Reported (NR) in the Conditions window severity column.

Conditions that have a default severity of Critical (CR), Major (MJ), Minor (MN), or Not-Alarmed (NA) but are not reported due to exclusion or suppression are shown as NR in the Conditions window.

Note For more information about alarm suppression, see the "DLP-B119 Suppress Alarm Reporting" section on page 6-30.

Current conditions are shown with the severity chosen in the alarm profile, if used. (For more information about alarm profiles, see the "NTP-B70 Create, Download, and Assign Alarm Severity Profiles" section on page 6-15.)

Note When ports are placed in OOS state for maintenance (OOS-MT), they raise the Alarms Suppressed for Maintenance (AS-MT) condition. For information about alarm and condition troubleshooting, refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 3 If you want to apply exclusion rules, check the **Exclude Same Root Cause** check box at the node or network view, but do not check the Exclude Same Root Cause check box in card view.

An exclusion rule eliminates all lower-level alarms or conditions that originate from the same cause. For example, a fiber break may cause an LOS alarm, an AIS condition, and an SF condition. If you check the Exclude Same Root Cause checkbox, only the LOS alarm will appear. According to Telcordia, exclusion rules apply to a query of "all conditions from a node."

Step 4 Return to your originating procedure (NTP).

NTP-B68 Delete Cleared Alarms from Display

Purpose	Use this procedure to delete Cleared (C) status alarms from the alarms window. The procedure can be used to delete transient messages from the CTC History window.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 Log into a node where you want to delete alarms. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. If you are already logged in, proceed to Step 2.

Step 2 To manually delete cleared node-level alarms:

a. In the node view, click the **Alarms** tab.

b. Refer to the rules in Step 8 and Click **Delete Cleared Alarms**.

This action removes any cleared ONS 15327 alarms from the Alarms display. The rows of cleared alarms turn white and have a C in their status (ST) column (Figure 6-5 on page 6-11).

Step 3 To automatically delete cleared alarms at the node level, check the **Autodelete Cleared Alarms** check box at the bottom-left of the window.

Step 4 To manually delete cleared card-level alarms:

a. In the node view, double-click the card graphic for the card you want to open.

b. Click the **Alarms** tab and click the **Delete Cleared Alarms** button, referring to the rules in Step 8.

Step 5 To automatically delete cleared alarms at the card level, check the **Autodelete Cleared Alarms** check box at the bottom-left of the window.

Step 6 To manually delete cleared network-level alarms:

a. In the node view click **View > Go to Network View**.

b. Click the **Alarms** tab and then, referring to the rules in Step 8, click **Delete Cleared Alarms**.

Step 7 If you want to automatically delete cleared alarms at the network level, check the **Autodelete Cleared Alarms** check box at the bottom-left of the window.

Step 8 Consult the following rules when deleting cleared alarms from the display:

- If the Autodelete Cleared Alarms check box is checked, an alarm disappears from the window when it is cleared.
- If the Autodelete Cleared Alarms check box is not checked, an alarm remains in the window after it is cleared. The alarm appears white in the window and has a Clear (CL) severity. The alarm can be removed by clicking the Delete Cleared Alarms button.

Step 9 Click **Delete Cleared Alarms** to remove the transient messages from the History window. Transient messages are single messages, and not raise-and-clear pairs (that is, they do not have companion messages stating they are cleared).

Stop. You have completed this procedure.

NTP-B69 View Alarm-Affected Circuits

Purpose	Use this procedure to view all circuits, if any, affected by an alarm or condition.
Tools/Equipment	None
Prerequisite Procedures	NTP-B196 View Alarms, History, Events, and Conditions, page 6-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

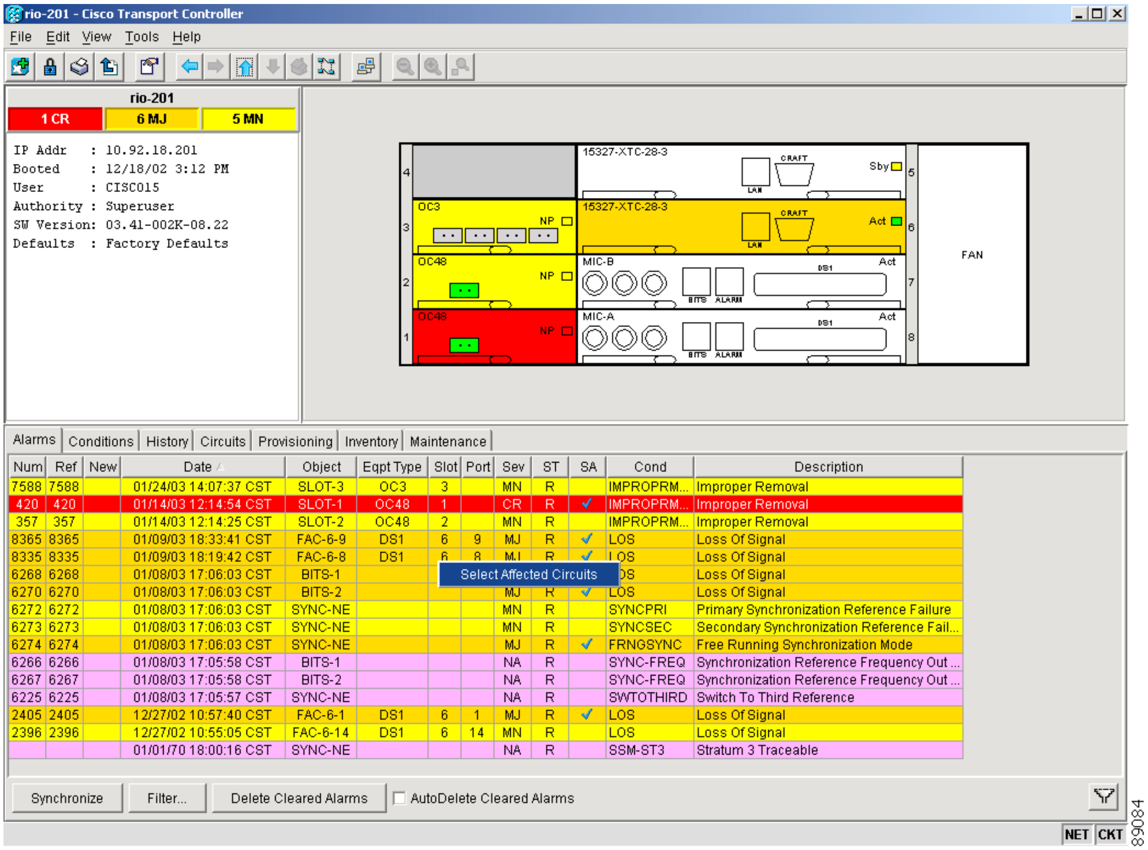
Step 2 In the network, node, or card view, click the **Alarms** tab or **Conditions** tab and then right-click anywhere in the row of an active alarm or condition.

Note The node view is the default, but you can also navigate to the Alarms tab in the network view or card view to perform Step 2.

Note The card view is not available for the MIC-A or MIC-B cards.

The Select Affected Circuit option appears on the shortcut menu (Figure 6-6).

Figure 6-6 Select Affected Circuits Option



rio-201

1 CR | 6 MJ | 5 MN

```
IP Addr   : 10.92.18.201
Booted    : 12/18/02 3:12 PM
User      : CISCO15
Authority : Superuser
SW Version: 03.41-002K-08.22
Defaults  : Factory Defaults
```

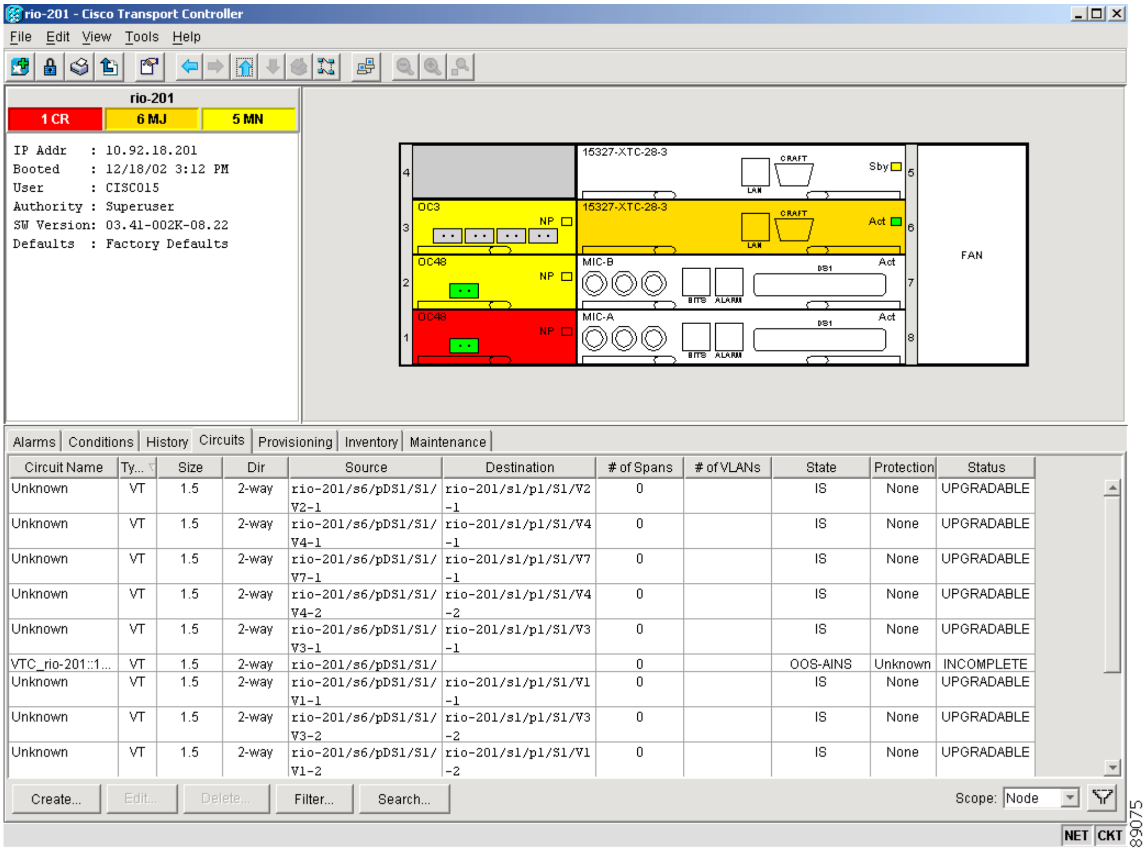
Num	Ref	New	Date	Object	Eqpt Type	Slot	Port	Sev	ST	SA	Cond	Description
7588	7588		01/24/03 14:07:37 CST	SLOT-3	OC3	3		MN	R		IMPROPRM...	Improper Removal
420	420		01/14/03 12:14:54 CST	SLOT-1	OC48	1		CR	R	✓	IMPROPRM...	Improper Removal
357	357		01/14/03 12:14:25 CST	SLOT-2	OC48	2		MN	R		IMPROPRM...	Improper Removal
8365	8365		01/09/03 18:33:41 CST	FAC-6-9	DS1	6	9	MJ	R	✓	LOS	Loss Of Signal
8335	8335		01/09/03 18:19:42 CST	FAC-6-8	DS1	6	8	MJ	R	✓	LOS	Loss Of Signal
6268	6268		01/08/03 17:06:03 CST	BITS-1				[illegible]	[illegible]	[illegible]	OS	Loss Of Signal
6270	6270		01/08/03 17:06:03 CST	BITS-2				MJ	R	✓	LOS	Loss Of Signal
6272	6272		01/08/03 17:06:03 CST	SYNC-NE				MN	R		SYNCPRI	Primary Synchronization Reference Failure
6273	6273		01/08/03 17:06:03 CST	SYNC-NE				MN	R		SYNCSEC	Secondary Synchronization Reference Fail...
6274	6274		01/08/03 17:06:03 CST	SYNC-NE				MJ	R	✓	FRNGSYNC	Free Running Synchronization Mode
6266	6266		01/08/03 17:05:58 CST	BITS-1				NA	R		SYNC-FREQ	Synchronization Reference Frequency Out ...
6267	6267		01/08/03 17:05:58 CST	BITS-2				NA	R		SYNC-FREQ	Synchronization Reference Frequency Out ...
6225	6225		01/08/03 17:05:57 CST	SYNC-NE				NA	R		SWTOTHIRD	Switch To Third Reference
2405	2405		12/27/02 10:57:40 CST	FAC-6-1	DS1	6	1	MJ	R	✓	LOS	Loss Of Signal
2396	2396		12/27/02 10:55:05 CST	FAC-6-14	DS1	6	14	MN	R		LOS	Loss Of Signal
			01/01/70 18:00:16 CST	SYNC-NE				NA	R		SSM-ST3	Stratum 3 Traceable

☐ AutoDelete Cleared Alarms

Step 3 Left-click or right-click **Select Affected Circuits**.

The Circuits window appears with the affected circuits highlighted (Figure 6-7).

Figure 6-7 Viewing an Alarm-Affected Circuit



```
IP Addr   : 10.92.18.201
Booted    : 12/18/02 3:12 PM
User      : CISCO15
Authority : Superuser
SW Version: 03.41-002K-08.22
Defaults  : Factory Defaults
```

Circuit Name	Ty...	Size	Dir	Source	Destination	# of Spans	# of VLANs	State	Protection	Status
Unknown	VT	1.5	2-way	rio-201/s6/pDS1/S1/V2-1	rio-201/s1/p1/S1/V2-1	0		IS	None	UPGRADABLE
Unknown	VT	1.5	2-way	rio-201/s6/pDS1/S1/V4-1	rio-201/s1/p1/S1/V4-1	0		IS	None	UPGRADABLE
Unknown	VT	1.5	2-way	rio-201/s6/pDS1/S1/V7-1	rio-201/s1/p1/S1/V7-1	0		IS	None	UPGRADABLE
Unknown	VT	1.5	2-way	rio-201/s6/pDS1/S1/V4-2	rio-201/s1/p1/S1/V4-2	0		IS	None	UPGRADABLE
Unknown	VT	1.5	2-way	rio-201/s6/pDS1/S1/V3-1	rio-201/s1/p1/S1/V3-1	0		IS	None	UPGRADABLE
VTC_rio-201::1...	VT	1.5	2-way	rio-201/s6/pDS1/S1/		0		OOS-AINS	Unknown	INCOMPLETE
Unknown	VT	1.5	2-way	rio-201/s6/pDS1/S1/V1-1	rio-201/s1/p1/S1/V1-1	0		IS	None	UPGRADABLE
Unknown	VT	1.5	2-way	rio-201/s6/pDS1/S1/V3-2	rio-201/s1/p1/S1/V3-2	0		IS	None	UPGRADABLE
Unknown	VT	1.5	2-way	rio-201/s6/pDS1/S1/V1-2	rio-201/s1/p1/S1/V1-2	0		IS	None	UPGRADABLE

Step 4 If you want to search for particular circuits, see the "DLP-B131 Search for Circuits" task on page 8-5.

Stop. You have completed this procedure.

NTP-B70 Create, Download, and Assign Alarm Severity Profiles

Purpose	Use this procedure to create a customized copy of the default alarm profile applied to a node, to download a saved custom profile from a network location to another node, to individually assign the custom severities to a port, card, or node, and to delete alarm profiles.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at the node where you want to create an alarm profile.If you are already logged in, continue with Step 2 to clone or modify an alarm profile, or continue with Step 3 to download an alarm profile.

Step 2 Complete the "DLP-B115 Create Alarm Severity Profiles" task on page 6-16. This task clones a current alarm profile, renames the profile, and customizes the new profile. Continue with Step 4.

Step 3 Complete the "DLP-B223 Download an Alarm Severity Profile" task on page 6-19. This task downloads an alarm severity profile from a CD or a node.

Step 4 As necessary, complete the "DLP-B116 Apply Alarm Profiles to Ports" task on page 6-20 or the "DLP-B117 Apply Alarm Profiles to Cards and Nodes" task on page 6-23.

Stop. You have completed this procedure.

DLP-B115 Create Alarm Severity Profiles

Purpose	Use this task to create a custom severity profile by modifying the default severity profile.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, choose **Go to Network View** from the View menu.

Step 2 Click the **Provisioning > Alarm Profiles** tabs (Figure 6-3 on page 6-6).

Step 3 Click **Load**.

Step 4 In the Select Profile(s) from Node or Filename to Load dialog box, click the **From Node** radio button.

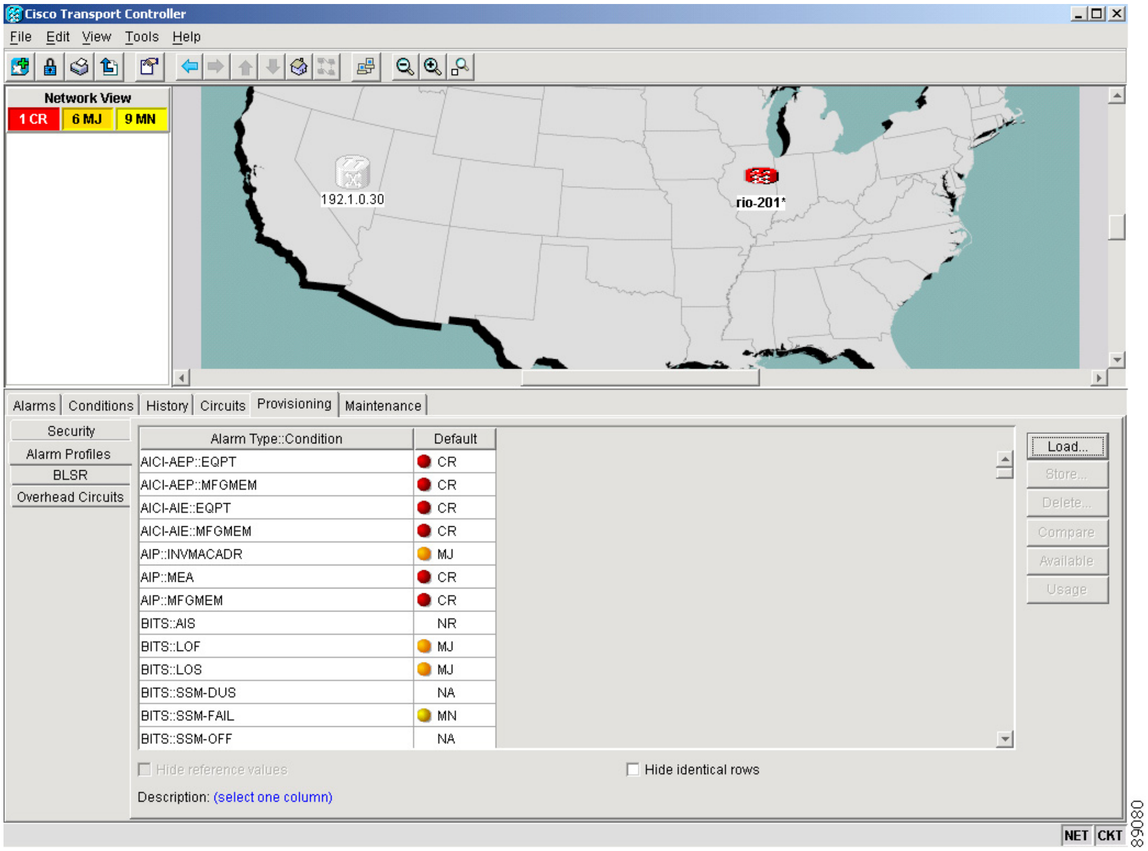
Step 5 Click the node name you are logged into in the Node Names list.

Step 6 Click **Default** to highlight this profile in the Profile Names list.

Step 7 Click **OK**.

The default alarm severity profile appears in the Alarm Profiles window (Figure 6-8).

Figure 6-8 Network View Alarm Profiles Window



Alarm Type::Condition	Default
AICI-AEP::EQPT	● CR
AICI-AEP::MFGMEM	● CR
AICI-AIE::EQPT	● CR
AICI-AIE::MFGMEM	● CR
AIP::INVMACADR	● MJ
AIP::MEA	● CR
AIP::MFGMEM	● CR
BITS::AIS	NR
BITS::LOF	● MJ
BITS::LOS	● MJ
BITS::SSM-DUS	NA
BITS::SSM-FAIL	● MN
BITS::SSM-OFF	NA

□ Hide reference values □ Hide identical rows

Description: (select one column)

Step 8 Right-click anywhere in the Default profile column to display the profile editing shortcut menu.

Step 9 Choose **Clone** from the shortcut menu.

Tip To identify profiles available for loading or cloning, click the Available button. You can clone any profiles except Inherited profiles.

Step 10 In the Clone Profile dialog box, enter a name for the copied profile in the New Profile Name field.

Profile names must be unique. If you try to import or name a profile that has the same name as another profile, CTC adds a suffix to create a new name. Long file names are supported (45 character maximum).

Step 11 Click **OK**.

A new alarm profile (named in Step 10) is created. This profile duplicates the default profile severities and appears to the right of the default profile in the Alarm Profiles window. You can highlight it and drag it to a different position.

Step 12 Modify (customize) the new alarm profile:

- **a.** In the new alarm profile column, double-click the alarm severity you want to change.
- **b.** Choose the desired severity in the Severity drop-down menu.
- **c.** Repeat Steps a and b for each severity you want to customize.

Step 13 After you have customized the new alarm profile, right-click the profile column to highlight it.

Step 14 Click **Store** in the profile editing shortcut menu.

Step 15 Click the **To Node(s)** radio button and continue with Step a or click the **To File** radio button and continue with Step b (Figure 6-9).

a. Choose the node(s) where you want to save the profile:

- If you want to save the profile to only one node, click the node in the Node Names list.
- If you want to save the profile to all nodes, click **Select All**.
- If you do not want to save the profile to any nodes, click **Select None**.
- If you want to update alarm profile information, click **Synchronize**.

b. Click **Browse** to navigate to the profile save location.

c. Enter a name in the file name field.

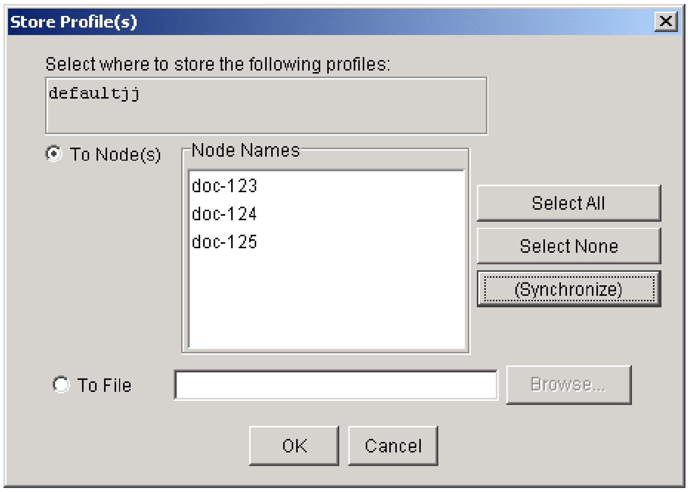
Long file names are supported. CTC supplies a suffix of *.pfl.

d. Click **OK**.

Note Click the Hide Identical Rows check box to configure the Alarm Profiles window to display rows with dissimilar severities.

Note Click the Hide Values Matching Profile Default check box to configure the Alarm Profiles window to display severities that do not match the Default profile.

Figure 6-9 Store Profile(s) Dialog Box



Store Profile(s)

Select where to store the following profiles:

defaulttjj

● To Node(s)

Node Names

doc-123
doc-124
doc-125

○ To File

Step 16 Return to your originating procedure (NTP).

DLP-B223 Download an Alarm Severity Profile

Purpose	Use this task to download a custom alarm severity profile from a network-drive accessible CD-ROM, floppy disk, or hard drive location.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, choose **Go to Network View** from the View menu (Figure 6-3 on page 6-6).

Step 2 Click the **Provisioning > Alarm Profiles** tabs.

Step 3 Click **Load**.

Step 4 If you want to download a file from the local PC hard drive, floppy disk, CD-ROM, or a network drive (if connected), click the **From File** radio button in the Select Profile(s) from Node or Filename to Load dialog box.

a. Click **Browse**.

The Open dialog box appears.

b. In the Look in drop-down menu, navigate to the folder where the profile file is located.

c. Click the name in the window to highlight it.

The file must have the *.pfl extension.

d. Click **Open**.

Continue with Step 6.

Step 5 If you want to download a file from the login node or another connected node, click the **From Node** radio button in the Select Profile(s) from Node or Filename to Load dialog box.

a. Click the node where the profile is located under the Node Names list.

b. Click the profile under the Profile Names list.

Step 6 Click **OK** in the Select Profile(s) from Node or Filename to Load dialog box.

The downloaded profile appears at the right side of the Alarm Profiles window.

Step 7 Right-click anywhere in the downloaded profile column to display the profile editing shortcut menu.

Step 8 Click **Store** in the shortcut menu.

Step 9 In the Store Profile(s) dialog box, click the **To Node(s)** radio button (Figure 6-9 on page 6-18).

a. Choose the node(s) where you want to save the profile:

- If you want to save the profile to only one node, click the node in the Node Names list.
- If you want to save the profile to all nodes, click **Select All**.
- If you do not want to save the profile to any nodes, click **Select None**.
- If you want to update alarm profile information, click **Synchronize**.

b. Click **OK**.

Step 10 Return to your originating procedure (NTP).

DLP-B116 Apply Alarm Profiles to Ports

Purpose	Use this task to apply a custom or default alarm severity profile to a port or ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-B115 Create Alarm Severity Profiles, page 6-16 DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 To change alarm profiles for optical cards, proceed to Step 2. To apply alarm profiles to optical card ports, proceed to Step 4. To apply alarm profiles to electrical card ports, proceed to Step 8.

Step 2 To change alarm profiles for optical cards, double-click an optical card in node view to display the card view.

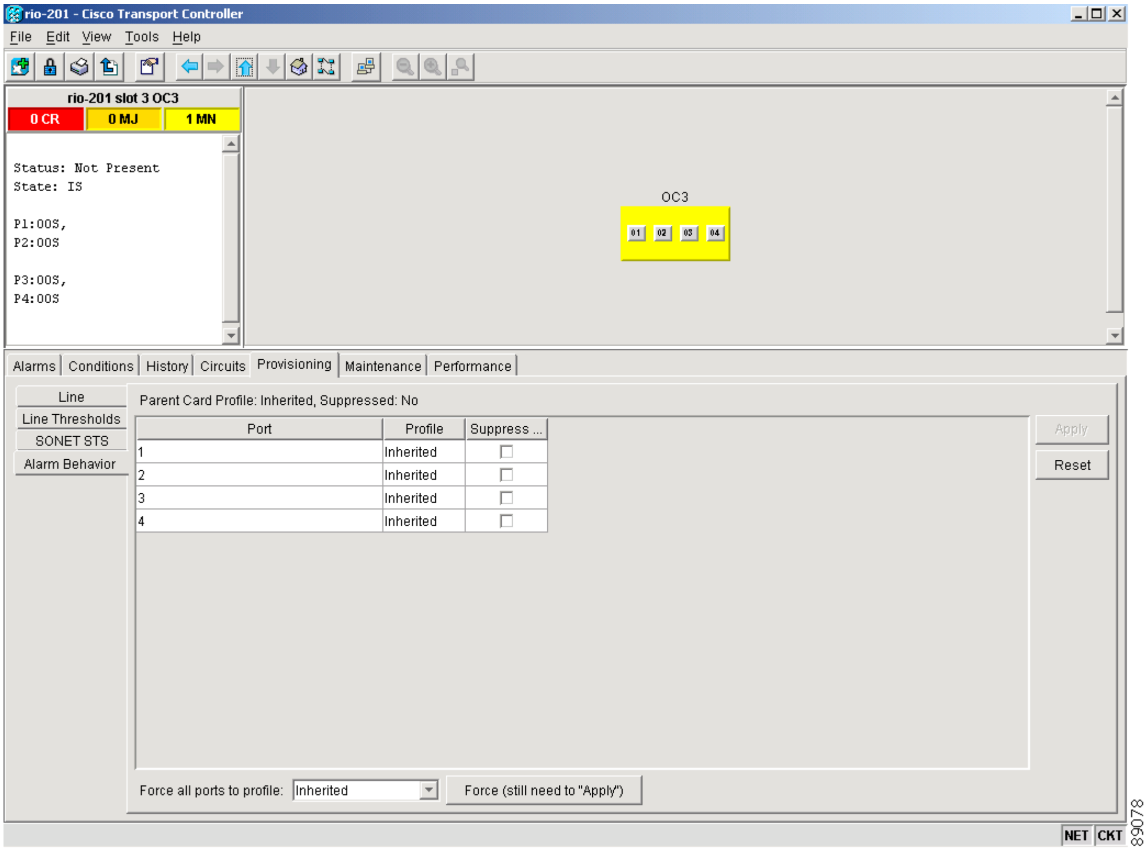
Note You can also apply alarm profiles to cards using the "DLP-B117 Apply Alarm Profiles to Cards and Nodes" task on page 6-23.

Note The card view is not available for the MIC-A or MIC-B cards.

Step 3 Click the **Provisioning > Alarm Behavior** tabs.

Figure 6-10 shows an alarm profile for OC-3 card ports. CTC shows Parent Card Profile: Inherited.

Figure 6-10 Card View Optical Port Alarm Profile


rio-201 - Cisco Transport Controller
File Edit View Tools Help
rio-201 slot 3 OC3
0 CR
0 MJ
1 MN
OC3
01 02 03 04
Alarms Conditions History Circuits Provisioning Maintenance Performance
Line
Line Thresholds
SONET STS
Alarm Behavior
Apply
Reset
Force (still need to "Apply")
NET CKT
89078

```
Status: Not Present
State: IS

P1:OOS,
P2:OOS

P3:OOS,
P4:OOS
```

Parent Card Profile: Inherited, Suppressed: No

Port	Profile	Suppress ...
1	Inherited	□
2	Inherited	□
3	Inherited	□
4	Inherited	□

Force all ports to profile: Inherited

Step 4 To apply alarm profiles to a port for optical cards:

a. Click the port row under the Profile column.

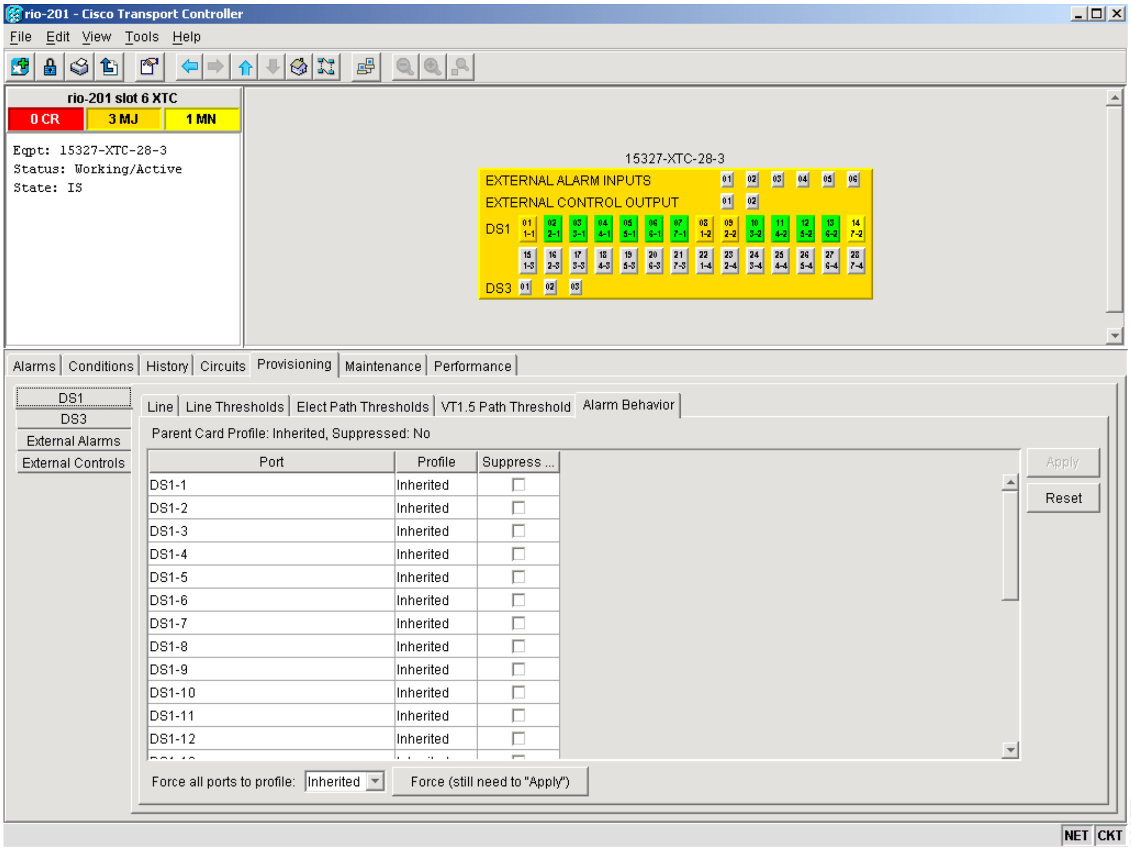
b. Choose the new profile from the Force all ports to profile drop-down menu.

c. Click **Apply**.

Step 5 To change alarm profiles for DS-1 and DS-3 ports, double-click the XTC card at the node (default login) view.

Step 6 Click the **Provisioning > DS1 > Alarm Behavior** tabs to change alarm profiles for DS-1 ports, or click the **Provisioning > DS3 > Alarm Behavior** tabs to change alarm profiles for DS-3 ports (Figure 6-11).

Figure 6-11 Card View Electrical Port Alarm Profile



Eqpt: 15327-XTC-28-3
Status: Working/Active
State: IS

Parent Card Profile: Inherited, Suppressed: No

Port	Profile	Suppress ...
DS1-1	Inherited	□
DS1-2	Inherited	□
DS1-3	Inherited	□
DS1-4	Inherited	□
DS1-5	Inherited	□
DS1-6	Inherited	□
DS1-7	Inherited	□
DS1-8	Inherited	□
DS1-9	Inherited	□
DS1-10	Inherited	□
DS1-11	Inherited	□
DS1-12	Inherited	□

Force all ports to profile: Inherited

Force (still need to "Apply")

Step 7 Repeat Step 5 for each DS-1 or DS-3 port where you want to change profiles.

Step 8 To apply profiles to all optical or electrical ports on a card:

a. Choose a new profile from the Force all ports to profile drop-down menu.

b. Click **Force (still need to "Apply")**.

c. Click **Apply**.

Tip If you choose the wrong profile, click **Reset** to return to the previous profile setting.

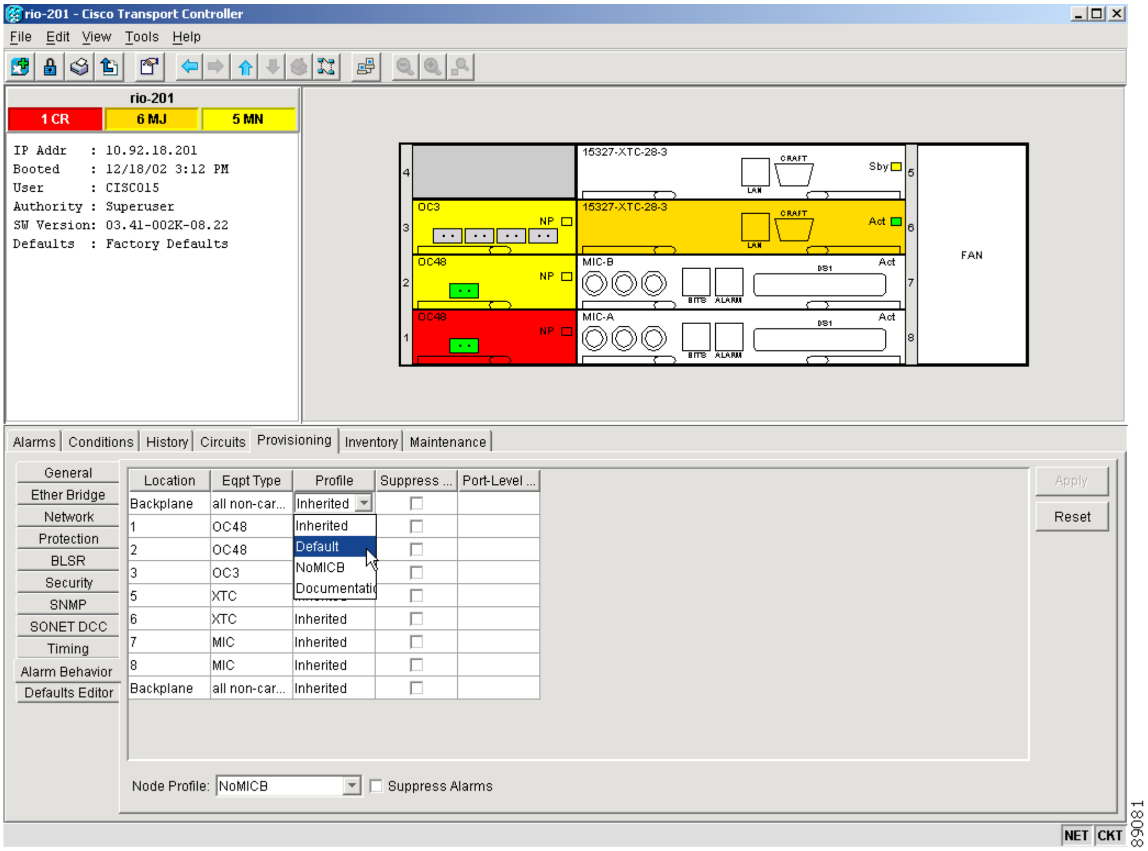
Step 9 Return to your originating procedure (NTP).

DLP-B117 Apply Alarm Profiles to Cards and Nodes

Purpose	Use this task to apply a custom or default alarm profile to cards or nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-B115 Create Alarm Severity Profiles, page 6-16 DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Alarm Behavior** tabs (Figure 6-12).

Figure 6-12 Node View Alarm Profile



rio-201 - Cisco Transport Controller

rio-201

1 CR 6 MJ 5 MN

```
IP Addr    : 10.92.18.201
Booted     : 12/18/02 3:12 PM
User       : CISCO15
Authority  : Superuser
SW Version: 03.41-002K-08.22
Defaults   : Factory Defaults
```

Location	Eqpt Type	Profile	Suppress ...	Port-Level ...
Backplane	all non-car...	Inherited	□	
1	OC48		□	
2	OC48		□	
3	OC3		□	
5	XTC		□	
6	XTC	Inherited	□	
7	MIC	Inherited	□	
8	MIC	Inherited	□	
Backplane	all non-car...	Inherited	□	

Node Profile: NoMICB □ Suppress Alarms

Step 2 To apply profiles to a card:

a. Click the Profile row for the card.

b. Choose the new profile from the Profile drop-down menu.

c. Click the **Apply** button.

Continue with Step 4.

Step 3 To apply the profile to an entire node:

a. Click the **Node Profile** menu arrow at the bottom of the window (Figure 6-12 on page 6-23).

b. Choose the new alarm profile in the **Profile** drop-down menu.

c. Click **Apply**.

Tip If you choose the wrong profile, click Reset to return to the previous profile.

Step 4 Return to your originating procedure (NTP).

DLP-B118 Delete Alarm Severity Profiles

Purpose	Use this task to delete a custom or default alarm severity profile.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, choose **Go to Network View** from the View menu.

Step 2 Click the **Provisioning > Alarm Profiles** tabs.

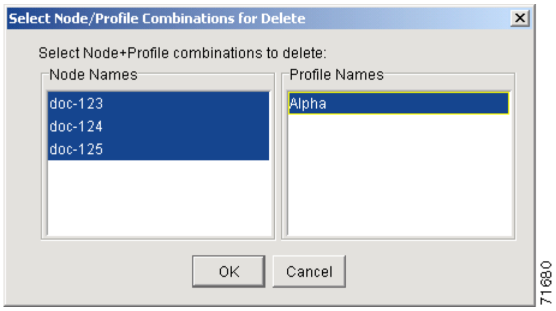
Step 3 Click the column heading for the profile column you want to delete (Figure 6-8 on page 6-17).

The selected alarm profile name is displayed in the Description field.

Step 4 Click **Delete**.

The Select Node/Profile Combination for Delete dialog box appears (Figure 6-13).

Figure 6-13 Select Node/Profile Combination For Delete Dialog Box



Select Node/Profile Combinations for Delete

Select Node+Profile combinations to delete:

Node Names	Profile Names
doc-123	Alpha
doc-124	
doc-125	

Step 5 Click the node name(s) in the Node Names list to highlight the profile location.

Tip If you hold the Shift key down, you can select consecutive node names. If you hold the Ctrl key down, you can select any combination of nodes.

Step 6 Click the profile name(s) you want to delete in the Profile Names list.

Step 7 Click **OK**.

The Delete Alarm Profile confirmation dialog box appears.

Step 8 Click **Yes** for each Delete Alarm Profile confirmation dialog box.

Note If you delete a profile from a node, it still appears in the network view Provisioning > Alarm Profiles window unless you remove it by choosing Remove.

Step 9 To remove the alarm profile from the Provisioning > Alarm Profiles window, right-click the column of the profile you deleted and choose **Remove** from the shortcut menu.

Note If a a node and profile combination is selected but does not exist, a warning appears: "One or more of the profile(s) selected do not exist on one or more of the node(s) selected." The profiles that do exist will be deleted.

Note The special profiles named Default and Inherited cannot be deleted and do not appear in the Select Node/Profile Combination for Delete Window.

Step 10 Return to your originating procedure (NTP).

NTP-B168 Enable, Modify, or Disable Alarm Severity Filtering

Purpose	Use this procedure to start, change, or stop alarm filtering for one or more severities in the Alarms, Conditions, and History windows in all network nodes.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

Step 2 As necessary, complete the "DLP-B225 Enable Alarm Filtering" task on page 6-26 to enable alarm filtering at the card, node, and network views for all nodes in the network. Alarm filtering can be enabled for alarms, conditions, or events.

Step 3 As necessary, complete the "DLP-B226 Modify Alarm and Condition Filtering Parameters" task on page 6-27 to modify the alarm filtering for network nodes to show or hide particular alarms or conditions.

Step 4 As necessary, complete the "DLP-B227 Disable Alarm Filtering" task on page 6-29 to disable alarm profile filtering for all network nodes.

Stop. You have completed this procedure.

DLP-B225 Enable Alarm Filtering

Purpose	Use this task to enable alarm filtering for alarms, conditions, or event history in all network nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 At the node, network, or card view, click the **Alarms** tab.

Step 2 Click the **Filter** tool at the lower-right side of the bottom toolbar.

Alarm filtering is enabled if the tool is selected and disabled if the tool is raised (not selected).

Alarm filtering will be enabled in the card, node, and network views of the Alarms tab at the node and for all other nodes in the network. If, for example, the Alarm Filter tool is enabled in the Alarms tab of the node view at one node, the Alarms tab in the network view and card view of that node will also show the tool enabled. All other nodes in the network will also have the tool enabled.

If you filter an alarm in card view, the alarm will still be displayed in node view. In this view, the card will display the color of the highest-level alarm. The alarm is also shown for the node in the network view.

Step 3 If you want alarm filtering enabled when you view conditions, repeat Steps 1 and 2 using the Conditions window.

Step 4 If you want alarm filtering enabled when you view alarm history, repeat Steps 1 and 2 using the History window.

Step 5 Return to your originating procedure (NTP).

DLP-B226 Modify Alarm and Condition Filtering Parameters

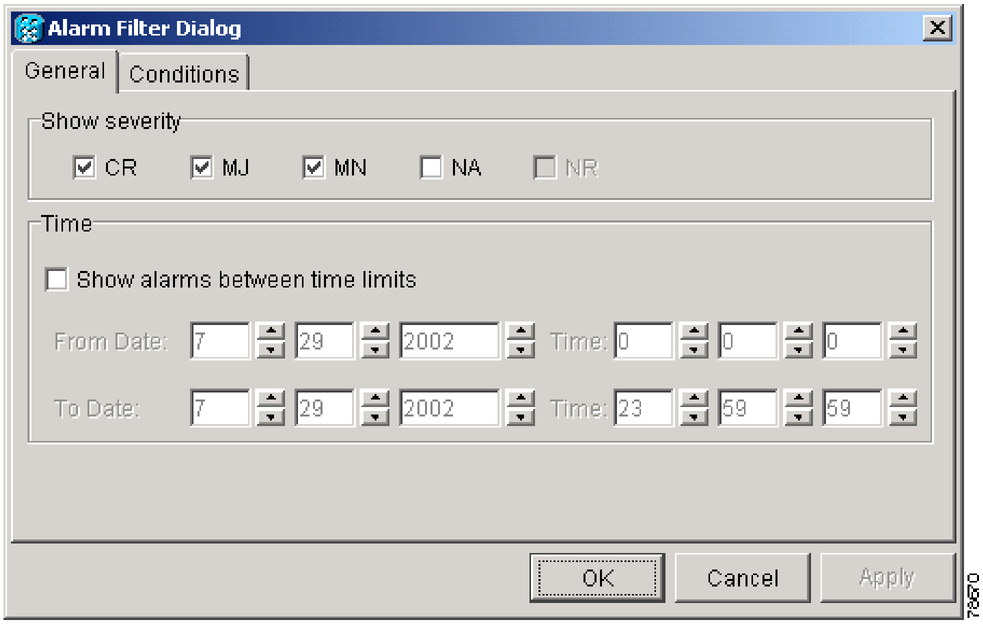
Purpose	Use this task change alarm and condition reporting in all network nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-B225 Enable Alarm Filtering, page 6-26 DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 At the node, network, or card view, click the **Alarms** tab.

Step 2 Click the **Filter** button at the lower-left of the bottom toolbar.

The Alarm Filter Dialog box appears, showing the General tab (Figure 6-14).

Figure 6-14 Alarm Filter Dialog Box General Tab


Alarm Filter Dialog
General
Conditions
Show severity
☑ CR
☑ MJ
☑ MN
□ NA
□ NR
Time
□ Show alarms between time limits
From Date: 7 29 2002 Time: 0 0 0
To Date: 7 29 2002 Time: 23 59 59
OK
Cancel
Apply
78670

In the General tab Show Severity area, you can choose which alarm severities will show through the alarm filter and provision a snapshot period during which alarms will appear. To change the alarm severities shown in the filter, continue with Step 3. To change the alarm time period, continue with Step 4.

Step 3 In the Show Severity area, click the check boxes for the severities [Critical (CR), Major (MJ*)*, Minor (MN), or Not-Alarmed (NA)] you want to be reported at the network level. Leave severity check boxes deselected (unchecked) to keep them from appearing.

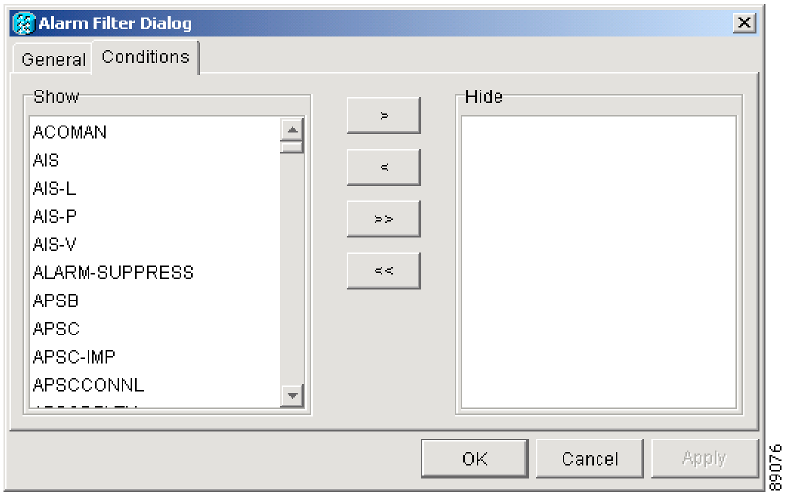
Note When alarm filtering is disabled, all alarms show.

Step 4 In the Time area, check the **Show alarms between time limits** check box to enable it. Then click the up and down arrows in the From Date, To Date, and Time fields to modify the time limits.

To modify filter parameters for conditions, continue with Step 5. If you do not need to modify them, continue with Step 6.

Step 5 Click the **Conditions** tab (Figure 6-15).

Figure 6-15 Alarm Filter Dialog Box Conditions Tab



When alarm filtering is enabled, conditions in the Show list are visible and conditions in the Hide list are invisible.

- To move conditions individually from the Show list to the Hide list, click the **>** button.
- To move conditions individually from the Hide list to the Show list, click the **<** button.
- To move conditions collectively from the Show list to the Hide list, click the **>>** button.
- To move conditions collectively from the Hide list to the Show list, click the **<<** button.

Note Conditions include alarms.

Step 6 Click **Apply** and **OK**.

Alarm and condition filtering parameters are enforced when alarm filtering is enabled (see the "DLP-B225 Enable Alarm Filtering" task on page 6-26), and are not enforced when alarm filtering is disabled (see the "DLP-B227 Disable Alarm Filtering" task on page 6-29).

Step 7 Return to your originating procedure (NTP).

DLP-B227 Disable Alarm Filtering

Purpose	Use this task to turn off specialized alarm filtering in all network nodes so that all severities are reported in CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-B225 Enable Alarm Filtering, page 6-26 DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 At the node, network, or card view, click the **Alarms** tab.

Step 2 Click the **Filter** tool at the lower-right side of the bottom toolbar.

Alarm filtering is enabled if the tool is selected and disabled if the tool is raised (not selected).

Step 3 If you want alarm filtering disabled when you view conditions, click the **Conditions** tab and repeat Step 2.

Step 4 If you want alarm filtering disabled when you view alarm history, click the **History** tab and repeat Step 2.

Step 5 Return to your originating procedure (NTP).

NTP-B72 Suppress and Discontinue Alarm Suppression

Purpose	Use this procedure to prevent alarms from being reported for a port, card, or node in circumstances when an alarm or condition is known to exist but you do not want to include in the display. Also use this procedure to resume normal alarm reporting by discontinuing the suppression.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, proceed to Step 2.

Step 2 Complete the "DLP-B119 Suppress Alarm Reporting" task on page 6-30 to make the node send out autonomous messages that clear particular raised alarms and cause the suppressed alarms to appear in the Conditions window.

Note Suppressing one or more alarms prevents them from appearing in Alarm or History windows or in any other clients. The suppress command causes CTC to display them in the Conditions window, where Not-Reported (NR) events are shown. The suppressed alarms appear there with the alarm severity they would have if they were reported; their severity color code, and service-affecting status.

Step 3 Complete the "DLP-B120 Discontinue Alarm Suppression" task on page 6-31 to remove the suppress-command and restore the alarms to their normal state of being reported at their provisioned severity.

Stop. You have completed this procedure.

DLP-B119 Suppress Alarm Reporting

Purpose	Use this task to suppress the reporting of ONS 15327 alarms at the port, card, or node level.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution If multiple CTC/TL1 sessions are open, suppressing alarms in one session suppresses the alarms in all other open sessions.

Step 1 At either the node or card view, click the **Provisioning > Alarm Behavior** tabs.

Step 2 To suppress alarms at the node level for optical cards, proceed to Step 3. To suppress alarms at the card level for optical ports, proceed to Step 5. To suppress alarms for electrical ports, proceed to Step 8.

Step 3 To suppress alarms at the node level for optical cards, check the **Suppress Alarms** column check box for the slot row where you want to suppress alarms (Figure 6-12 on page 6-23).

Note In the node view, row numbers correspond to slot numbers.

Step 4 Click **Apply**.

The node sends out autonomous messages to clear any raised alarms.

Step 5 To suppress alarms at the card level for optical ports, double-click the card and click the **Provisioning > Alarm Behavior** tabs.

Step 6 Click the **Suppress Alarms** column check box for the optical port row where you want to suppress alarms (Figure 6-10 on page 6-21).

Step 7 Click **Apply**.

Step 8 To suppress alarms for DS-1 or DS-3 ports, double-click the XTC card graphic at the node view.

Step 9 To suppress DS-1 port alarms, click the **Provisioning > DS1 > Alarm Behavior** tabs. To suppress DS-3 port alarms, click the **Provisioning > DS3 > Alarm Behavior** tabs (Figure 6-11 on page 6-22).

Step 10 Check the **Suppress Alarms** column check box for each port where you want to enable alarm reporting.

Step 11 Return to your originating procedure (NTP).

DLP-B120 Discontinue Alarm Suppression

Purpose	Use this task to discontinue alarm suppression and reenable alarm reporting on a port, card, or node.
Tools/Equipment	None
Prerequisite Procedures	DLP-B119 Suppress Alarm Reporting, page 6-30 DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view click the **Provisioning > Alarm Behavior** tabs. To discontinue suppression for optical cards, proceed to Step 2. To discontinue suppression for electrical ports, proceed to Step 4.

Note You must restore alarm reporting at the view where it was originally suppressed.

Step 2 To discontinue alarm suppression at the node level for optical cards, uncheck the **Suppress Alarms** check box at the lower-left of the Alarm Behavior window.

Step 3 Click **Apply**.

Step 4 To discontinue alarm suppression at the card level for optical ports, double-click the card to display the card view.

Step 5 Uncheck the **Suppress Alarms** check box for the port(s) you no longer want to suppress.

Step 6 Click **Apply**.

Step 7 To discontinue alarm suppression for DS-1 or DS-3 ports, double-click the XTC card graphic at the node view.

Step 8 To discontinue DS-1 port alarm suppression, click the **Provisioning > DS1 > Alarm Behavior** tabs. To discontinue DS-3 port alarm suppression, click the **Provisioning > DS3 > Alarm Behavior** tabs.

Step 9 Uncheck the **Suppress Alarms** column check box for each port where you want to discontinue alarm reporting.

Step 10 Return to your originating procedure (NTP).

NTP-B32 Provision External Alarms and Controls on the XTC

Purpose	Use this procedure to create external (environmental) alarms and external controls.
Tools/Equipment	An XTC card must be installed in Slot 5 or 6.
Prerequisite Procedures	NTP-B24 Verify Card Installation, page 3-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note For information about the XTC external alarms and controls, virtual wire and orderwire, refer to the *Cisco ONS 15327 Reference Guide*.

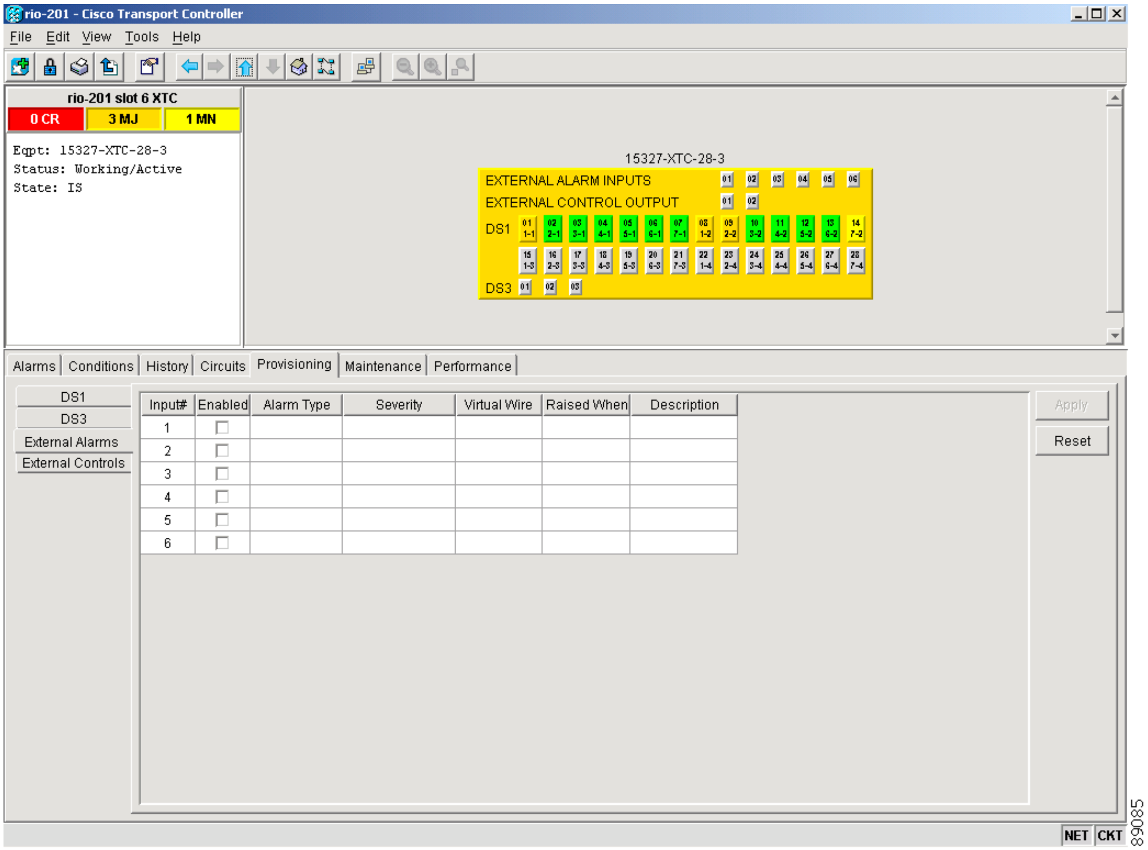
Note External alarm physical connections are made on the MIC. However, the alarms are provisioned using the XTC card view.

Step 1 In the node view, double-click the active XTC card. The card view appears.

Step 2 If you are provisioning external alarms, click the **Provisioning > External Alarms** tabs (Figure 6-16). If you are not provisioning external alarms, continue with Step 6.

Note You can only provision external alarms on the active XTC card.

Figure 6-16 XTC Card External Alarms



```
Eqpt: 15327-XTC-28-3
Status: Working/Active
State: IS
```

Input#	Enabled	Alarm Type	Severity	Virtual Wire	Raised When	Description
1	□					
2	□					
3	□					
4	□					
5	□					
6	□					

Step 3 Complete the following fields for each external device wired to the Mechanical Interface card (MIC):

- Enabled—Check this check box to activate the fields for the alarm input number.
- Alarm Type—Choose an option from the Alarm Type drop-down menu.
- Severity—Choose an option from the Severity drop-down menu.

  The severity determines the severity the alarm has in the Alarms and History tabs and determines whether the LEDs are activated. Critical (CR), Major (MJ), and Minor (MN) alarms activate the XTC LEDs. Not-Alarmed (NA) and Not-Reported (NR) do not activate LEDs, but do report the information in CTC.
- Virtual Wire—Choose an option to assign the external device to a virtual wire. Otherwise, do not change the None default. For information about the virtual wire, see the *Cisco ONS 15327 Reference Manual*.
- Raised When—Choose the condition (open or closed) that triggers the alarm.
- Description—A default description is provided; enter a different description if needed.

Step 4 To provision up to six virtual wire inputs for external devices, complete Step 3 for each additional device.

Step 5 Click **Apply**.

Step 6 If you are provisioning external control outputs for external devices, click the **External Controls** subtab (Figure 6-16).

Step 7 Complete the following fields for each external control wired to the MIC:

- Enabled—Check this the check box to activate the Control Type, Trigger Type, and Description columns for the alarm input number.
- Control Type—Choose an option: air conditioner, engine, fan, generator, heat, light, sprinkler, or miscellaneous.
- Trigger Type—Choose a trigger type: a local minor, major, or critical alarm; a remote minor, major, or critical alarm; or a virtual wire activation.
- Description—Enter a description.

Step 8 To provision a second external control, complete Step 7 for the additional device.

Step 9 Click **Apply**.

Stop. You have completed this procedure.

CHAPTER 7

Monitor Performance

Performance monitoring (PM) parameters are used by service providers to gather, store, threshold, and report performance data for early detection of problems. For more PM information, details, and definitions refer to the *Cisco ONS 15327 Reference Manual*. This chapter explains how to enable and view performance monitoring statistics for the Cisco ONS 15327.

Before You Begin

Before performing any of the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15327 Troubleshooting Guide* as necessary.

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-B73 Enable Performance Monitoring, page 7-2—Complete as needed.
2. NTP-B195 Monitor Electrical or Optical Performance, page 7-6—Complete as needed.
3. NTP-B198 Monitor Ethernet Performance, page 7-15—Complete as needed.

Note For additional information regarding PM parameters, refer to the Digital transmission surveillance section in Telcordia's GR-1230-CORE, GR-820-CORE, GR-499-CORE, and GR-253-CORE documents, and in the ANSI document entitled *Digital Hierarchy - Layer 1 In-Service Digital Transmission Performance Monitoring*.

NTP-B73 Enable Performance Monitoring

Purpose	This procedure describes how to enable performance monitoring.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As Needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at the node you want to monitor. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-B121 Enable Pointer Justification Count Performance Monitoring" task on page 7-2 if you need to monitor clock synchronization.

Step 3 Complete the "DLP-B122 Enable Intermediate-Path Performance Monitoring" task on page 7-4 if you need to monitor large amounts of STS traffic through intermediate nodes.

Stop. You have completed this procedure.

DLP-B121 Enable Pointer Justification Count Performance Monitoring

Purpose	This task enables pointer justification counts, which provide a way to align the phase variations in STS and VT payloads and to monitor the clock synchronization between nodes. A consistent, large pointer justification count indicates clock synchronization problems between nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the card where the line terminates (drops), called a line-terminating equipment (LTE) card. The card view appears.

Table 7-1 lists the Cisco ONS 15327 LTE cards.

Table 7-1 Traffic Cards that Terminate the Line (LTEs)

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

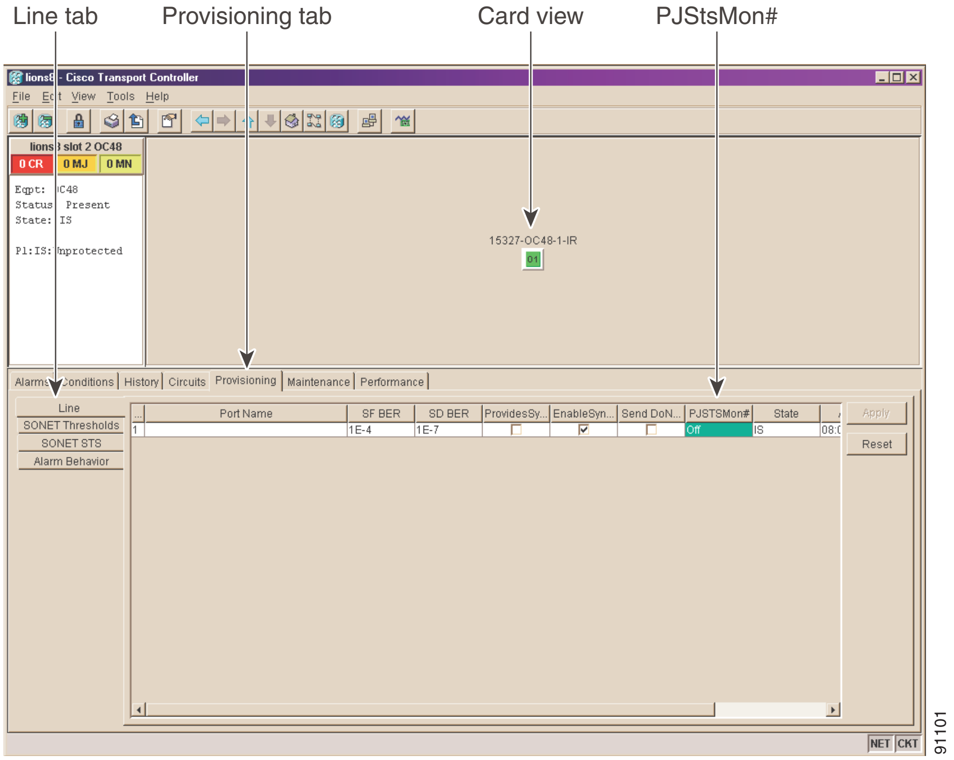
Step 2 Click the **Provisioning > Line** tabs.

Step 3 Click the PJStsMon# menu and make a selection based on the following rules.

- The default value Off means pointer justification monitoring is disabled.
- The values 1 to N are the number of STSs on the port. One STS per port can be enabled from the PJStsMon# card menu.

Figure 7-1 shows the PJStsMon# menu on the Provisioning window.

Figure 7-1 Line Tab for Enabling Pointer Justification Count Parameters



Eqpt: OC48
Status Present
State: IS

P1:IS: Unprotected

...	Port Name	SF BER	SD BER	ProvidesSy...	EnableSyn...	Send DoN...	PJSTSMon#	State	/
1		1E-4	1E-7	□	☑	□	Off	IS	08:(

Step 4 In the State field, confirm that the port is in service (IS).

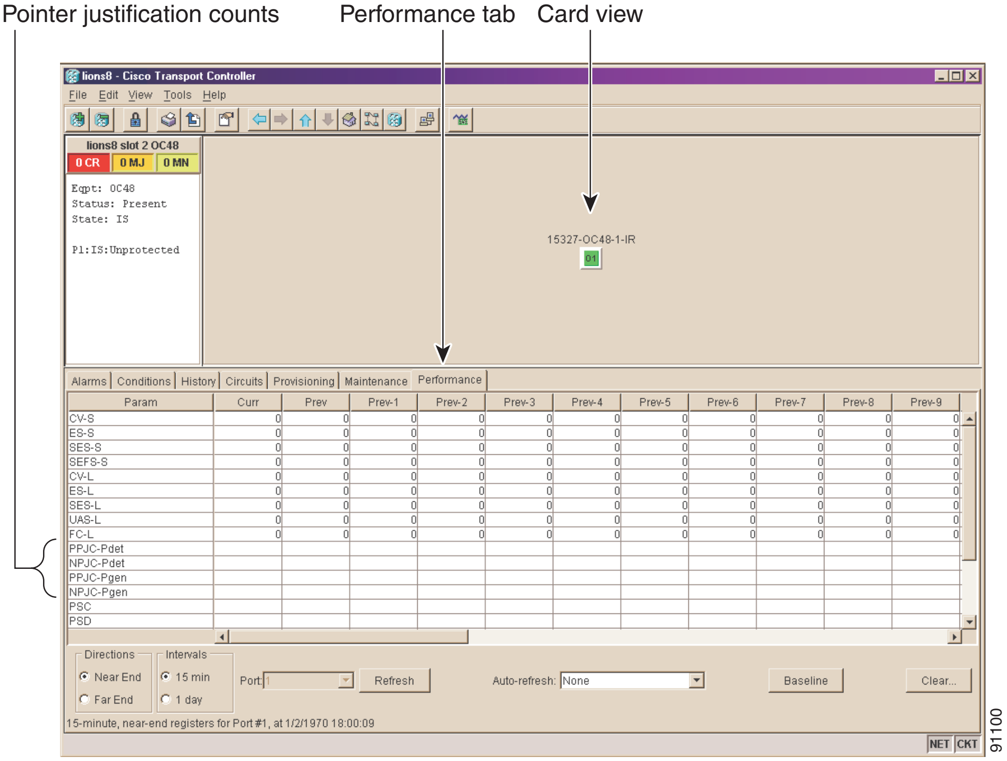
Step 5 If the port is IS, click **Apply** and go to Step 7.

Step 6 If the port is out of service (OOS, OOS_MT, OOS_AINS), select **IS** in the State field and click **Apply**.

Step 7 Click the **Performance** tab to view PM parameters. Figure 7-2 shows pointer justification counts. Refer to the *Cisco ONS 15327 Reference Manual* for more PM information, details, and definitions.

Note On CTC, the count fields for PPJC and NPJC PM parameters appear white and blank unless they are enabled on the Provisioning > Line tabs.

Figure 7-2 Viewing Pointer Justification Counts



```
Eqpt: OC48
Status: Present
State: IS

P1:IS:Unprotected
```

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Prev-9
CV-S	0	0	0	0	0	0	0	0	0	0	0
ES-S	0	0	0	0	0	0	0	0	0	0	0
SES-S	0	0	0	0	0	0	0	0	0	0	0
SEFS-S	0	0	0	0	0	0	0	0	0	0	0
CV-L	0	0	0	0	0	0	0	0	0	0	0
ES-L	0	0	0	0	0	0	0	0	0	0	0
SES-L	0	0	0	0	0	0	0	0	0	0	0
UAS-L	0	0	0	0	0	0	0	0	0	0	0
FC-L	0	0	0	0	0	0	0	0	0	0	0
PPJC-Pdet											
NPJC-Pdet											
PPJC-Pgen											
NPJC-Pgen											
PSC											
PSD											

Directions: ● Near End ○ Far End

Intervals: ● 15 min ○ 1 day

Port: 1

Auto-refresh: None

15-minute, near-end registers for Port #1, at 1/2/1970 18:00:09

Step 8 Return to your originating procedure (NTP).

DLP-B122 Enable Intermediate-Path Performance Monitoring

Purpose	This task enables intermediate-path performance monitoring, which allows you to monitor large amounts of STS traffic through intermediate nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The monitored IPPM parameters are STS CV-P, STS ES-P, STS SES-P, STS UAS-P, and STS FC-P. For more information about IPPM parameters, refer to the *Cisco ONS 15327 Reference Manual*.

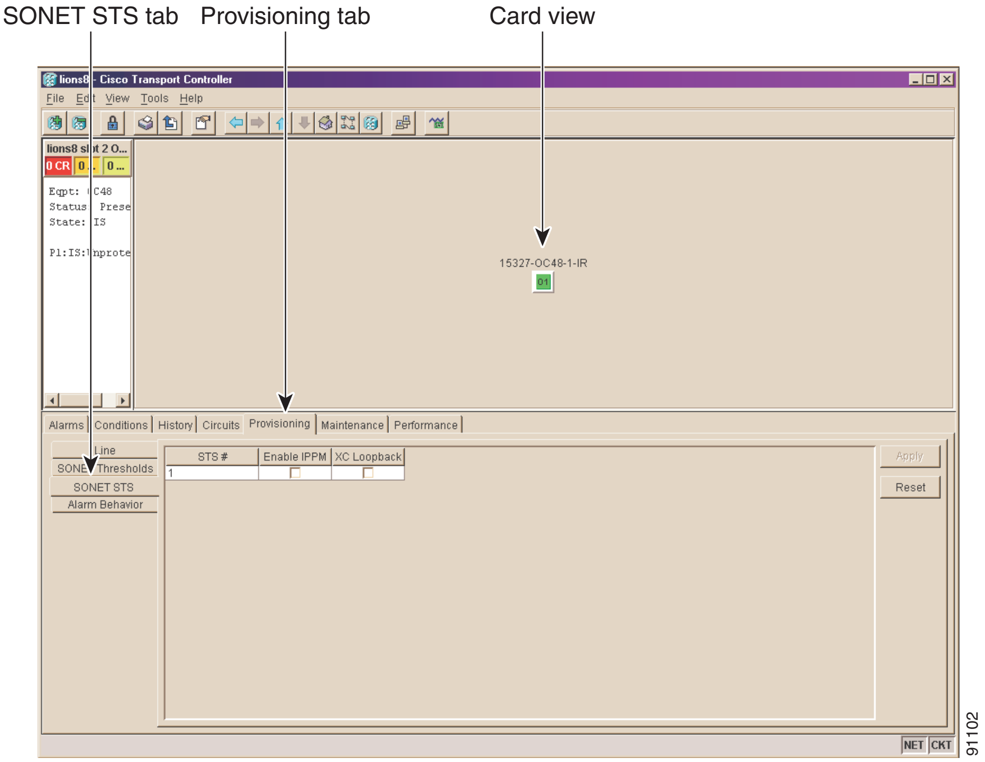
Step 1 In node view, double-click the LTE card you want to monitor. The card view appears.

See Table 7-1 on page 7-2 for a list of Cisco ONS 15327 LTE cards.

Step 2 Click the **Provisioning** tab**.**

Step 3 Click the **SONET STS** tab. Figure 7-3 shows the SONET STS tab on the Provisioning window.

Figure 7-3 SONET STS Tab for Enabling IPPM



STS #	Enable IPPM	XC Loopback
1	□	□

Step 4 Check the check box in the Enable IPPM column for the STS you want to monitor.

Step 5 Click **Apply** button.

Step 6 Click the **Performance** tab to view PM parameters. For IPPM parameter definitions, refer to the *Cisco ONS 15327 Reference Manual*.

Step 7 Return to your originating procedure (NTP).

NTP-B195 Monitor Electrical or Optical Performance

Purpose	The Performance Monitoring window allows you to view node near-end or far-end performance on a selected card and port at specified time intervals to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	Before you monitor performance, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 5, "Create Circuits and VT Tunnels" and Chapter 9, "Change Port Settings."
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at the node you want to monitor. If you are already logged in, continue to Step 2.

Step 2 Complete the "DLP-B123 View Electrical PM Parameters" task on page 7-7 as needed.

Step 3 As needed, use the following tasks to change the display of electrical PM counts:

- DLP-B261 Refresh PM Counts for a Different Port, page 7-8
- DLP-B124 Refresh Electrical or Optical PM Counts at Fifteen-Minute Intervals, page 7-8
- DLP-B318 Refresh Electrical or Optical PM Counts at One-Day Intervals, page 7-9
- DLP-B126 Monitor Near-End PM Counts, page 7-10
- DLP-B127 Monitor Far-End PM Counts, page 7-10
- DLP-B129 Reset Current PM Counts, page 7-11
- DLP-B130 Clear Selected PM Counts, page 7-11
- DLP-B260 Set Auto-Refresh Interval for Displayed PM Counts, page 7-12

Step 4 Complete the "DLP-B317 View Optical OC-N PM Parameters" task on page 7-13 as needed.

Step 5 As needed, use the following tasks to change the display of optical PM counts:

- DLP-B261 Refresh PM Counts for a Different Port, page 7-8
- DLP-B124 Refresh Electrical or Optical PM Counts at Fifteen-Minute Intervals, page 7-8
- DLP-B318 Refresh Electrical or Optical PM Counts at One-Day Intervals, page 7-9
- DLP-B126 Monitor Near-End PM Counts, page 7-10
- DLP-B127 Monitor Far-End PM Counts, page 7-10
- DLP-B319 Monitor PM Counts for Selected Signal Types, page 7-14
- DLP-B129 Reset Current PM Counts, page 7-11
- DLP-B130 Clear Selected PM Counts, page 7-11
- DLP-B260 Set Auto-Refresh Interval for Displayed PM Counts, page 7-12

Stop. You have completed this procedure.

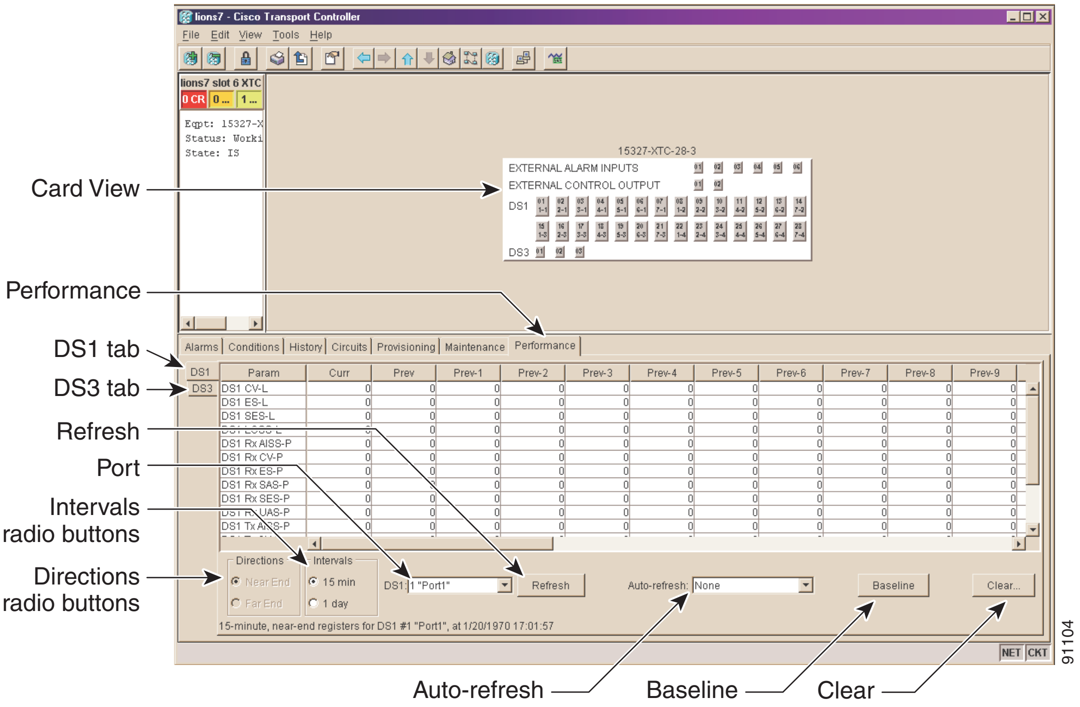
DLP-B123 View Electrical PM Parameters

Purpose	This task enables you to view DS-1 or DS-3 PM counts on a selected XTC card to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click an XTC card. The card view appears.

Step 2 Click the **Performance** tab (Figure 7-4).

Figure 7-4 Viewing Electrical Performance Monitoring Information



Eqpt: 15327-X
Status: Worki
State: IS

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Prev-9
DS1 CV-L	0	0	0	0	0	0	0	0	0	0	0
DS1 ES-L	0	0	0	0	0	0	0	0	0	0	0
DS1 SES-L	0	0	0	0	0	0	0	0	0	0	0
DS1 LOSS-L	0	0	0	0	0	0	0	0	0	0	0
DS1 Rx AISS-P	0	0	0	0	0	0	0	0	0	0	0
DS1 Rx CV-P	0	0	0	0	0	0	0	0	0	0	0
DS1 Rx ES-P	0	0	0	0	0	0	0	0	0	0	0
DS1 Rx SAS-P	0	0	0	0	0	0	0	0	0	0	0
DS1 Rx SES-P	0	0	0	0	0	0	0	0	0	0	0
DS1 Rx UAS-P	0	0	0	0	0	0	0	0	0	0	0
DS1 Tx AISS-P	0	0	0	0	0	0	0	0	0	0	0

Directions: ● Near End ○ Far End
Intervals: ● 15 min ○ 1 day
DS1: 1 "Port1"
Auto-refresh: None

15-minute, near-end registers for DS1 #1 "Port1", at 1/20/1970 17:01:57

Step 3 Click the **DS1** or **DS3** tab to view the desired PM parameters.

The PM parameter names appear on the left portion of the window in the Param column. The PM values appear on the right portion of the window in the Curr (current), and Prev-*n* (previous) columns. For PM parameter definitions, refer to the *Cisco ONS 15327 Reference Manual*.

Step 4 Return to your originating procedure (NTP).

DLP-B261 Refresh PM Counts for a Different Port

Purpose	This task changes the window view to display PM counts for another port on a multiport card.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click an XTC card (for electrical PM counts) or OC-N card. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 From the Port drop-down menu choose the desired port to highlight your selection.

Step 4 Click the **Refresh** button. The PM counts for the newly selected port appear.

Step 5 Return to your originating procedure (NTP).

DLP-B124 Refresh Electrical or Optical PM Counts at Fifteen-Minute Intervals

Purpose	This task changes the window view to display PM counts in 15-minute intervals.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click an XTC card (for electrical PM counts) or OC-N card. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **15 min** radio button.

Step 4 Click the **Refresh** button. Performance monitoring parameters appear in 15-minute intervals synchronized with the time of day.

Step 5 View the Curr column to find PM counts for the current 15-minute interval.

Each monitored performance parameter has corresponding threshold values for the current time period. If the value of the counter exceeds the threshold value for a particular 15-minute interval, a threshold crossing alert (TCA) is raised. The PM number represents the counter value for each specific performance monitoring parameter.

Step 6 View the Prev-*n* columns to find PM counts for the previous 15-minute intervals.

Note If a complete 15-minute interval count is not possible, the value appears with a yellow background. An incomplete or incorrect count can be caused by monitoring for less than 15 minutes after the counter started, changing node timing settings, changing the time zone settings, replacing a card, resetting a card, or by changing port states. When the problem is corrected, the subsequent 15-minute interval appears with a white background.

Step 7 Return to your originating procedure (NTP).

DLP-B318 Refresh Electrical or Optical PM Counts at One-Day Intervals

Purpose	This task changes the window to display PM parameters in 1-day intervals.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click an XTC card (for electrical PM counts) or OC-N card. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **1 day** radio button.

Step 4 Click **Refresh**. Performance monitoring appears in 1-day intervals synchronized with the time of day.

Step 5 View the Curr column to find PM counts for the current 1-day interval.

Each monitored performance parameter has corresponding threshold values for the current time period. If the value of the counter exceeds the threshold value for a particular 1-day interval, a threshold crossing alert (TCA) is raised. The PM number represents the counter value for each performance monitoring parameter.

Step 6 View the Prev-*n* columns to find PM counts for the previous 1-day intervals.

Note If a complete count over a 1-day interval is not possible, the value appears with a yellow background. An incomplete or incorrect count can be caused by monitoring for less than 24 hours after the counter started, changing node timing settings, changing the time zone settings, replacing a card, resetting a card, or by changing port states. When the problem is corrected, the subsequent 1-day interval appears with a white background.

Step 7 Return to your originating procedure (NTP).

DLP-B126 Monitor Near-End PM Counts

Purpose	Use this task to view near-end PM counts for the selected card and port.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click an XTC card (for electrical PM counts) or OC-N card. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **Near End** radio button.

Step 4 Click the **Refresh** button. All PM parameters for the selected card on the incoming signal appear. For PM parameter definitions refer to the *Cisco ONS 15327 Reference Manual*.

Step 5 View the Curr column to find PM counts for the current time interval.

Step 6 View the Prev-*n* columns to find PM counts for the previous time intervals.

Step 7 Return to your originating procedure (NTP).

DLP-B127 Monitor Far-End PM Counts

Purpose	Use this task to view far-end PM parameters for the selected card and port.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click an XTC card (for electrical PM counts) or OC-N card. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **Far End** radio button.

Note Only cards that allow far-end performance monitoring have this button as an option.

Step 4 Click the **Refresh** button. All PM parameters recorded by the far-end node for the selected card on the outgoing signal appear. For PM parameter definitions refer to the *Cisco ONS 15327 Reference Manual*.

Step 5 View the Curr column to find PM counts for the current time interval.

Step 6 View the Prev-*n* columns to find PM counts for the previous time intervals.

Step 7 Return to your originating procedure (NTP).

DLP-B129 Reset Current PM Counts

Purpose	This task uses the Baseline button to clear the PM count displayed in the current time interval, but it does not clear the cumulative PM count. This task allows you to see how quickly PM counts rise.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click an XTC card (for electrical PM counts), Ethernet card, or OC-N card. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click **Baseline**.

Note The Baseline button clears the PM counts displayed in the current time interval, but does not clear the PM counts on the card. When the current time interval expires or the window view changes, the total number of PM counts on the card and in the window appear in the appropriate column. The baseline values are discarded if you change views to a different window and then return to the Performance Monitoring window.

Step 4 View the current statistics column(s) to observe changes to PM counts for the current time interval.

Step 5 Return to your originating procedure (NTP).

DLP-B130 Clear Selected PM Counts

Purpose	This task uses the Clear button to clear specified PM counts depending on the option selected.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Caution Pressing the Clear button can mask problems if used incorrectly. This button is commonly used for testing purposes.

Step 1 In node view, double-click an Ethernet card, XTC card (for electrical PM counts), or OC-N card. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click **Clear**.

Step 4 From the Clear Statistics menu, choose one of three options:

- Selected statistics: Clearing selected statistics erases from the card and the window display all PM counts associated with the current combination of statistics on the selected port. This means the selected time interval, direction, and signal type counts are erased from the card and the window display.
- All statistics on port x: Clearing all statistics on port x erases from the card and the window display all PM counts associated with all combinations of the statistics on the selected port. This means all time intervals, directions, and signal type counts are erased from the card and the window display.
- All statistics in current view: Clearing all statistics in the current view erases from the card and the window display all PM counts for all ports.

Step 5 From the Clear Statistics menu, click **Yes** to clear the selected statistics.

Step 6 View the displayed columns to verify that the selected PM counts have been cleared.

Step 7 Return to your originating procedure (NTP).

DLP-B260 Set Auto-Refresh Interval for Displayed PM Counts

Purpose	This task changes the window auto-refresh intervals for updating the displayed PM counts.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click an Ethernet card, XTC card (for electrical PM counts), or OC-N card. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the Auto-refresh drop-down menu button.

Step 4 Choose one of six options:

- None: This option disables the auto-refresh feature.
- 15 Seconds: This option sets the window auto-refresh to 15-second time intervals.
- 30 Seconds: This option sets the window auto-refresh to 30-second time intervals.
- 1 Minute: This option sets the window auto-refresh to 1-minute time intervals.
- 3 Minutes: This option sets the window auto-refresh to 3-minute time intervals.
- 5 Minutes: This option sets the window auto-refresh to 5-minute time intervals.

Step 5 Click the **Refresh** button. The PM counts for the newly-selected auto-refresh time interval appear.

Depending on the selected auto-refresh interval, the displayed PM counts automatically update when each refresh interval completes. If the auto-refresh interval is set to None, the displayed PM counts are not updated unless you click the Refresh button.

Step 6 Return to your originating procedure (NTP).

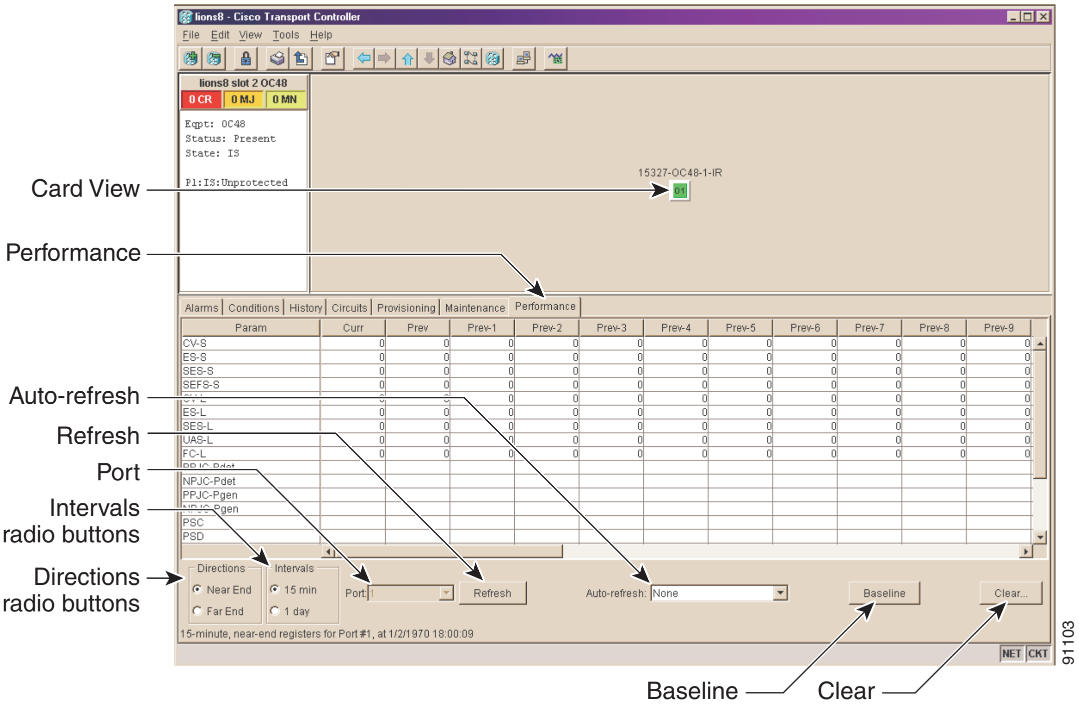
DLP-B317 View Optical OC-N PM Parameters

Purpose	This task enables you to view PM counts on a selected optical (OC-N) card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click an OC-N card. The card view appears.

Step 2 Click the **Performance** tab (Figure 7-4 on page 7-7).

Figure 7-5 Viewing Optical Performance Monitoring Information



```
Eqpt: OC48
Status: Present
State: IS

P1:IS:Unprotected
```

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Prev-9
CV-S	0	0	0	0	0	0	0	0	0	0	0
ES-S	0	0	0	0	0	0	0	0	0	0	0
SES-S	0	0	0	0	0	0	0	0	0	0	0
SEFS-S	0	0	0	0	0	0	0	0	0	0	0
CV-L	0	0	0	0	0	0	0	0	0	0	0
ES-L	0	0	0	0	0	0	0	0	0	0	0
SES-L	0	0	0	0	0	0	0	0	0	0	0
UAS-L	0	0	0	0	0	0	0	0	0	0	0
FC-L	0	0	0	0	0	0	0	0	0	0	0
PPJC-Pdet											
NPJC-Pdet											
PPJC-Pgen											
NPJC-Pgen											
PSC											
PSD											

Directions: ● Near End ○ Far End
Intervals: ● 15 min ○ 1 day
Port: 1
Auto-refresh: None

15-minute, near-end registers for Port #1, at 1/2/1970 18:00:09

The PM parameter names appear on the left portion of the window in the Param column. The PM values appear on the right portion of the window in the Curr (current), and Prev-*n* (previous) columns. For PM parameter definitions, refer to the *Cisco ONS 15327 Reference Manual*.

Step 3 Return to your originating procedure (NTP).

DLP-B319 Monitor PM Counts for Selected Signal Types

Purpose	Use the signal-type menus to monitor near-end or far-end PM counts for specific signals on a selected card and port.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click an XTC card (for electrical PM counts) or OC-N card. The card view appears.

Step 2 Click the **Performance** tab.

Note Different port and signal-type menus appear depending on the card type and the circuit type. The appropriate types (DS1, DS3, VT path, STS path, OC-N section and line) appear based on the card. For example, the OC-48 card lists the OC-48 port and STS path PM parameters as signal-types. You can select both the OC-48 port and the STS within the specified OC-48.

Step 3 Click the Port/Line drop-down menu button and highlight the desired port/line. (Options vary depending on the card.)

Step 4 Click the signal type drop-down menu button and highlight the desired signal. (Options vary depending on the card.)

Step 5 Click the **Refresh** button. All PM counts recorded by the near-end or far-end node appear for the specified outgoing signal type on the selected card and port. For PM parameter definitions, refer to the *Cisco ONS 15327 Reference Manual*.

Step 6 View the Curr column to find PM counts for the current time interval.

Step 7 View the Prev-*n* columns to find PM counts for the previous time intervals.

Step 8 Return to your originating procedure (NTP).

NTP-B198 Monitor Ethernet Performance

Purpose	This procedure allows you to view node transmit and receive performance on an Ethernet card and port at specified time intervals to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	Before you monitor performance, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 5, "Create Circuits and VT Tunnels" and Chapter 9, "Change Port Settings."
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at the node you want to monitor. If you are already logged in, continue with Step 2.

Step 2 Complete the "DLP-B256 View Ethernet Statistics PM Parameters" task on page 7-16 as needed.

Step 3 As needed, use the following tasks to change the display of Ethernet statistical PM counts:

- DLP-B260 Set Auto-Refresh Interval for Displayed PM Counts, page 7-12
- DLP-B129 Reset Current PM Counts, page 7-11
- DLP-B130 Clear Selected PM Counts, page 7-11

Step 4 Complete the "DLP-B257 View Ethernet Utilization PM Parameters" task on page 7-17 as needed.

Step 5 As needed, use the "DLP-B259 Refresh Ethernet PM Counts at a Different Time Interval" task on page 7-18 to change the display of Ethernet utilization PM counts:

Step 6 Complete the "DLP-B258 View Ethernet History PM Parameters" task on page 7-18 as needed.

Step 7 As needed, use the following tasks to change the display of Ethernet history PM counts:

- DLP-B261 Refresh PM Counts for a Different Port, page 7-8
- DLP-B259 Refresh Ethernet PM Counts at a Different Time Interval, page 7-18

Stop. You have completed this procedure.

DLP-B256 View Ethernet Statistics PM Parameters

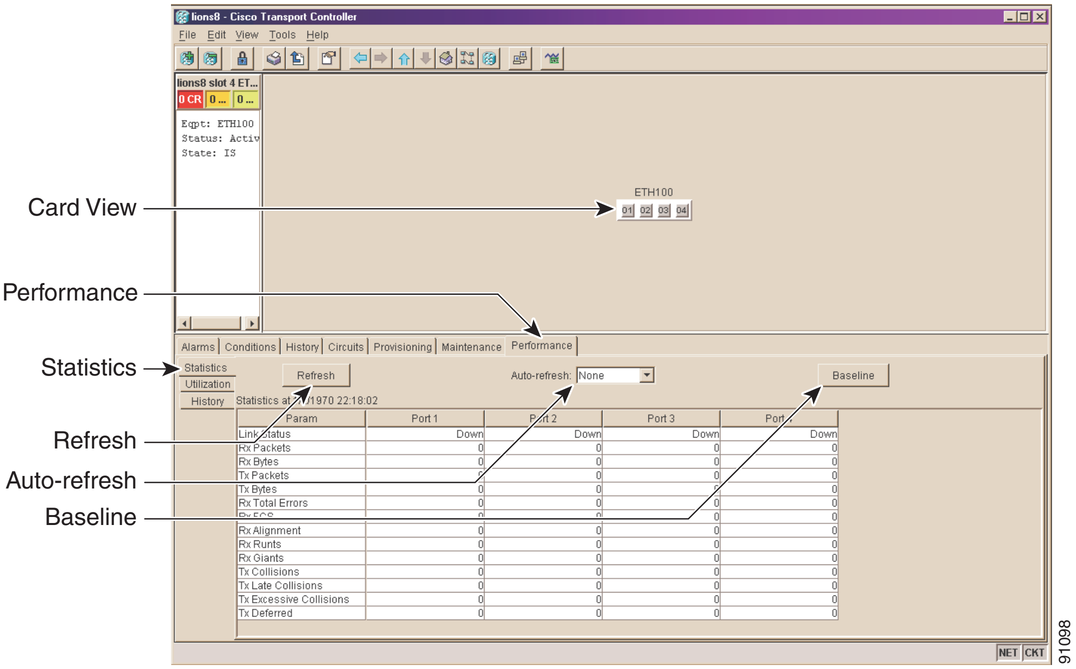
Purpose	This task enables you to view current statistical PM counts on a selected E-Series or G-Series Ethernet card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click an E-Series or G-Series Ethernet card. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **Statistics** subtab (Figure 7-6).

Figure 7-6 Statistics Window on the Card View Performance Tab



Eqpt: ETH100
Status: Activ
State: IS

Statistics at [illegible]/1970 22:18:02

Param	Port 1	Port 2	Port 3	Port 4
Link Status	Down	Down	Down	Down
Rx Packets	0	0	0	0
Rx Bytes	0	0	0	0
Tx Packets	0	0	0	0
Tx Bytes	0	0	0	0
Rx Total Errors	0	0	0	0
Rx FCS	0	0	0	0
Rx Alignment	0	0	0	0
Rx Runts	0	0	0	0
Rx Giants	0	0	0	0
Tx Collisions	0	0	0	0
Tx Late Collisions	0	0	0	0
Tx Excessive Collisions	0	0	0	0
Tx Deferred	0	0	0	0

Step 4 Click the **Refresh** button. Performance monitoring statistics for each port on the card appear.

The PM parameter names appear on the left portion of the window in the Param column. The parameter numbers appear on the right portion of the window in the Port # columns. For PM parameter definitions refer to the *Cisco ONS 15327 Reference Manual*.

Step 5 View the Port # columns to see the current PM statistics for each port.

Step 6 Return to your originating procedure (NTP).

DLP-B257 View Ethernet Utilization PM Parameters

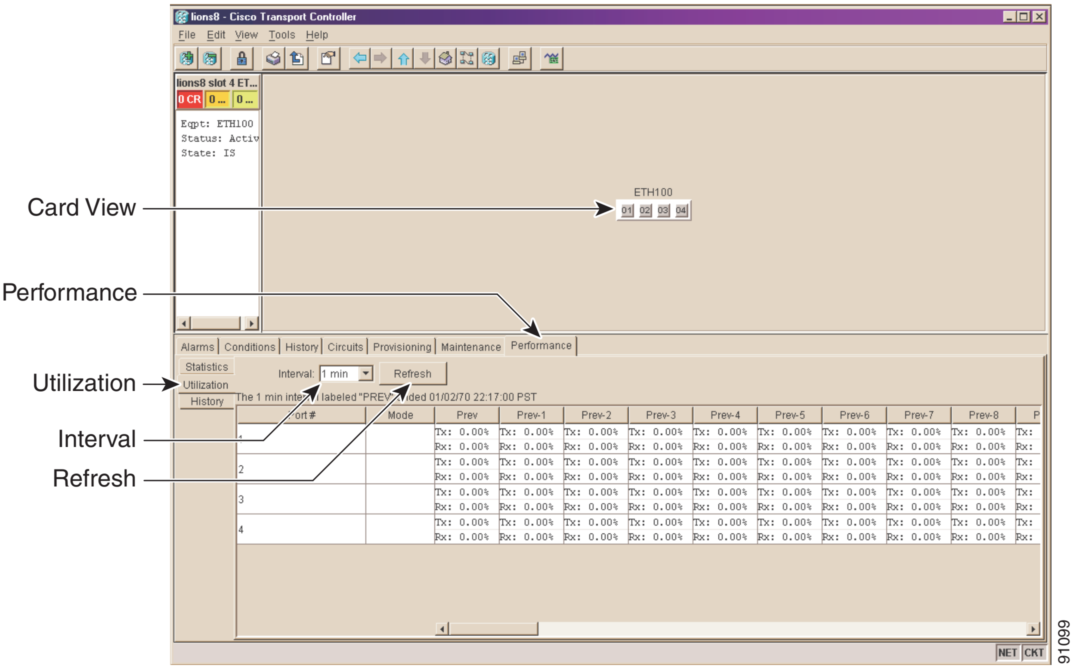
Purpose	This task enables you to view line utilization PM counts on a selected E-Series or G-Series Ethernet card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click an E-Series or G-Series Ethernet card. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **Utilization** subtab (Figure 7-7).

Figure 7-7 Utilization Window on the Card View Performance Tab



Eqpt: ETH100
Status: Activ
State: IS

Interval: 1 min

The 1 min interval labeled "PREV" ended 01/02/70 22:17:00 PST

Port #	Mode	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	P
1		Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: Rx:
2		Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: Rx:
3		Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: Rx:
4		Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: 0.00% Rx: 0.00%	Tx: Rx:

Step 4 Click the **Refresh** button. Performance monitoring utilization values for each port on the card appear.

Step 5 View the Port # column to find the port you want to monitor.

Step 6 View the Prev-*n* columns to find Tx and Rx bandwidth utilization values for the previous time intervals.

Step 7 Return to your originating procedure (NTP).

DLP-B259 Refresh Ethernet PM Counts at a Different Time Interval

Purpose	This task changes the window view to display specified PM counts in time intervals depending on the interval option selected.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click an E-Series or G-Series Ethernet card. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **Utilization** tab or the **History** tab.

Step 4 Click the Interval drop-down menu button.

Step 5 Choose one of four options:

- **1 min**: This option displays the specified PM counts in one-minute time intervals.
- **15 min**: This option displays the specified PM counts in fifteen-minute time intervals.
- **1 hour**: This option displays the specified PM counts in one-hour time intervals.
- **1 day**: This option displays the specified PM counts in one-day (24 hours) time intervals.

Step 6 Click the **Refresh** button. The PM counts refresh with values based on the chosen time interval.

Step 7 Return to your originating procedure (NTP).

DLP-B258 View Ethernet History PM Parameters

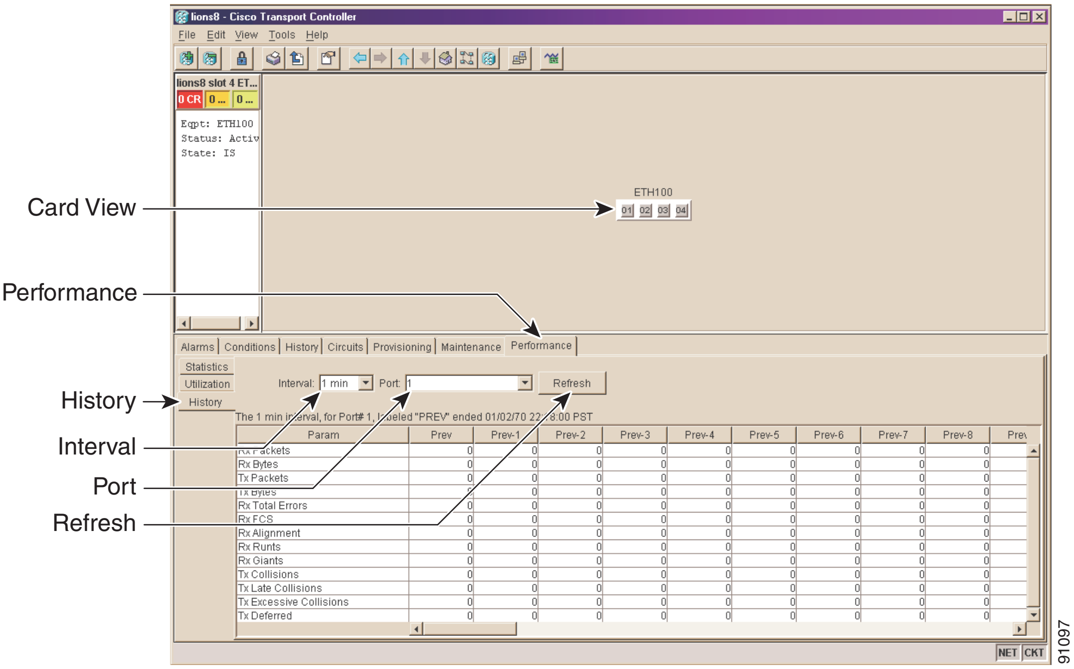
Purpose	This task enables you to view historical PM counts at selected time intervals on an E-Series or G-Series Ethernet card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click an E-Series or G-Series Ethernet card. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **History** subtab (Figure 7-8).

Figure 7-8 History Window on the Card View Performance Tab



Interval: 1 min Port: 1

The 1 min interval, for Port# 1, labeled "PREV" ended 01/02/70 22:18:00 PST

Param	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Prev
Rx Packets	0	0	0	0	0	0	0	0	0	
Rx Bytes	0	0	0	0	0	0	0	0	0	
Tx Packets	0	0	0	0	0	0	0	0	0	
Tx Bytes	0	0	0	0	0	0	0	0	0	
Rx Total Errors	0	0	0	0	0	0	0	0	0	
Rx FCS	0	0	0	0	0	0	0	0	0	
Rx Alignment	0	0	0	0	0	0	0	0	0	
Rx Runts	0	0	0	0	0	0	0	0	0	
Rx Giants	0	0	0	0	0	0	0	0	0	
Tx Collisions	0	0	0	0	0	0	0	0	0	
Tx Late Collisions	0	0	0	0	0	0	0	0	0	
Tx Excessive Collisions	0	0	0	0	0	0	0	0	0	
Tx Deferred	0	0	0	0	0	0	0	0	0	

Step 4 Click the **Refresh** button. Performance monitoring statistics for each port on the card appear.

The PM parameter names appear on the left portion of the window in the Param column. The parameter numbers appear on the right portion of the window in the Port # columns. For PM parameter definitions refer to the *Cisco ONS 15327 Reference Manual*.

Step 5 View the Port # columns to see the current PM statistics for each port.

Step 6 Return to your originating procedure (NTP).

CHAPTER 8

Manage Circuits

This chapter explains how to manage Cisco ONS 15327 electrical, optical, and Ethernet circuits.

Before You Begin

To create circuits, see Chapter 5, "Create Circuits and VT Tunnels."

To clear any alarm or trouble conditions, refer to the *Cisco ONS 15327 Troubleshooting Guide*.

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-B199 Locate and View Circuits, page 8-3—Complete as needed.
2. NTP-B151 Modify Circuit Characteristics, page 8-7—Complete as needed.
3. NTP-B151 Modify Circuit Characteristics, page 8-7—Complete as needed to edit a circuit name, change the active and standby colors of spans, or change signal fail thresholds, signal degrade thresholds, reversion time, and PDI-P settings for UPSR circuits.
4. NTP-B416 Convert a CTC Circuit to TL1 Cross-Connects, page 8-11—Complete this procedure if you want to convert a CTC circuit into TL1 cross-connects.
5. NTP-B417 Upgrade TL1 Cross-Connects to CTC Circuits, page 8-13—Complete this procedure if you want to convert TL1 cross-connects or TL1-like cross-connects created in CTC into a CTC circuit.
6. NTP-B152 Delete Circuits, page 8-13—Complete as needed.
7. NTP-B78 Create a Monitor Circuit, page 8-14—Complete as needed to monitor traffic on primary bidirectional circuits.
8. NTP-B79 Create a J1 Path Trace, page 8-15—Complete as needed to monitor interruptions or changes to circuit traffic.

The Cisco Transport Controller Circuits window displays information about circuits to help you manage the circuits, including circuit status and state. Table 8-1 lists the statuses that CTC can report for each circuit.

Table 8-1 ONS 15327 Circuit Status

Status	Definition/Activity
CREATING	CTC is creating a circuit.
ACTIVE	CTC created a circuit. All components are in place and a complete path exists from the circuit source to the circuit destination.
DELETING	CTC is deleting a circuit.
INCOMPLETE	A CTC-created circuit is missing a cross-connect or network span; a complete path from source to destination(s) does not exist. In CTC, circuits are represented using cross-connects and network spans. If a network span is missing from a circuit, the circuit status is INCOMPLETE. However, an INCOMPLETE status does not necessarily mean a circuit traffic failure has occurred, because traffic can flow on a protect path. Network spans are in one of two states: up or down. In CTC circuit and network maps, up spans are displayed as green lines, and down spans are displayed as gray lines. If a failure occurs on a network span during a CTC session, the span remains on the network map but its color changes to gray. If you restart your CTC session while the failure is active, the new CTC session cannot discover the span and its span line will not display on the network map. Subsequently, circuits routed on a network span that goes down will display as ACTIVE during the current CTC session, but they will display as INCOMPLETE to users who log in after the span failure.
UPGRADABLE	A TL1-created circuit or a TL1-like CTC-created circuit is complete and has upgradable cross-connects. A complete path from source to destination(s) exists. CTC can create an active circuit.
INCOMPLETE_UPGRADABLE	A TL1-created circuit or a TL1-like CTC-created circuit with upgradable cross-connects is missing a cross-connect, and a complete path from source to destination(s) does not exist. The circuit cannot be upgraded until missing cross-connects are in place.

Table 8-1 ONS 15327 Circuit Status (continued)

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

Circuit state, shown in Table 8-2, is a user-assigned, administrative status that defines whether the circuit is in or out of service. To carry circuit traffic, circuits must have a status of active and a state of in service (IS).

Table 8-2 ONS 15327 Circuit States

State	Definition
IS	In service; able to carry traffic
OOS	Out of service; unable to carry traffic
OOS-AINS	Out of service, auto in service; alarm reporting is suppressed, but traffic is carried and loopbacks are allowed. Raised fault conditions, whether their alarms are reported or not, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command. VT circuits generally switch to IS when source and destination ports are IS, OOS_AINS, or OOS_MT regardless of whether a physical signal is present. STS circuits switch to IS when a signal is received.
OOS-MT	Out of service, maintenance; alarm reporting is suppressed, but traffic is carried and loopbacks are allowed. Raised fault conditions, whether their alarms are reported or not, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command.

NTP-B199 Locate and View Circuits

Purpose	This procedure provides tasks that you can use to locate and view ONS 15327 circuits.
Tools/Equipment	None
Prerequisite Procedures	Circuit creation procedure(s) in Chapter 5, "Create Circuits and VT Tunnels"
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Log into the network where you want to view the circuits. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "DLP-B131 Search for Circuits" task on page 8-5.

Step 3 As needed, complete the "DLP-B262 Filter the Display of Circuits" task on page 8-4.

Step 4 As needed, complete the "DLP-B229 View Circuits on a Span" task on page 8-6.

Stop. You have completed this procedure.

DLP-B262 Filter the Display of Circuits

Purpose	This task filters the display of circuits in the ONS 15327 network, node, or card view Circuits window based on circuit name, size, type, direction, and other attributes.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Navigate to the appropriate CTC view:

- To filter network circuits, from the View menu choose **Go to Network View**.
- To filter circuits that originate, terminate, or pass through a specific node, from the View menu. choose **Go to Other Node**, then choose the node you want to search and click **OK**.
- To filter circuits that originate, terminate, or pass through a specific card, double-click the card on the shelf graphic in node view to display the card in card view.

Step 2 Click the **Circuits** tab.

Step 3 Set the attributes for filtering the circuit display:

a. Click the **Filter** button.

b. On the Filter Dialog, set the filter attributes:

- Name—Enter a complete or partial circuit name to filter circuits based on circuit name; otherwise leave the field blank.
- Direction—Choose one: **Any** (direction not used to filter circuits), **1-way** (display only one-way circuits), or **2-way** (display only two-way circuits).
- Status—Choose one: **Any** (status not used to filter circuits), **Active** (display only active circuits), **Incomplete** (display only incomplete circuits, that is, circuits missing a connection or span to form a complete path), or **Upgradable** (display only upgradable circuits, that is, circuits created in TL1 that are ready to upgrade in CTC). See Table 8-1 for more information about circuit statuses. Although other statuses are described in Table 8-1, filtering is only supported for Active, Incomplete, and Upgradable circuits.
- State—Choose one: **OOS** (display only out-of-service circuits), **IS** (display only inservice circuits), **OOS-AINS** (display only out of service, auto inservice circuits), or **OOS-MT** (display only out of service, maintenance circuits.) See Table 8-2 for more information about circuit states.

- Slot—Enter a slot number to filter circuits based on the source or destination slot; otherwise leave the field blank.
- Port—Enter a port number to filter circuits based on the source or destination port; otherwise leave the field blank.
- Type—Choose one: **Any** (type not used to filter circuits), **STS** (displays only STS circuits), **VT** (displays only VT circuits), or **VT Tunnel** (displays only VT tunnels).
- Size—Click the appropriate check boxes to filter circuits based on size: VT1.5, STS-1, STS3c, STS-6c, STS-9c, STS-12c, STS-24c, STS-48c. The check boxes that appear depend on what you entered in the Type field. If you chose Any, all sizes are available. If you chose VT, only VT1.5 is available. If you chose STS, only STS sizes are available, and if you chose VT Tunnel or VT Aggregation Point, only STS-1 is available.

Step 4 Click **OK**. Circuits matching the attributes in the Filter Circuits dialog box appear in the Circuits window.

Step 5 To turn filtering off, click the Filter icon in the lower right corner of the Circuits window. Click the icon again to turn filtering on, and click the Filter button to change the filter attributes.

Step 6 Return to your originating procedure (NTP).

DLP-B131 Search for Circuits

Purpose	This task searches for an ONS 15327 circuit at the network, node, or card level.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Navigate to the appropriate CTC view:

- To search the entire network, from the View menu choose **Go to Network View**.
- To search for circuits that originate, terminate, or pass through a specific node, from the View menu choose **Go to Other Node**, then choose the node you want to search and click **OK**.
- To search for circuits that originate, terminate, or pass through a specific card, double-click the card on the shelf graphic in node view to display the card in card view.

Step 2 Click the **Circuits** tab.

Step 3 If you are in node or card view, choose the scope for the search in the Scope drop-down menu.

Step 4 Click **Search**.

Step 5 In the Circuit Name Search dialog box, complete the following:

- Find What—Enter the text of the circuit name you want to find.
- Match Whole Word Only—Select this check box to instruct CTC to select circuits only if the entire word matches the text in the Find What field.

- Match Case—Select this check box to instruct CTC to select circuits only when the capitalization matches the capitalization entered in the Find What field.
- Direction—Choose the direction for the search. Searches are conducted up or down from the currently selected circuit.

Step 6 Click **Find Next**. If a match is found, click **Find Next** again to find the next circuit.

Step 7 Repeat Steps 5and 6 until you are finished, then click **Cancel**.

Step 8 Return to your originating procedure (NTP).

DLP-B229 View Circuits on a Span

Purpose	This task displays circuits routed on an ONS 15327 span.
Tools/Equipment	None
Prerequisite Procedures	Circuits must be created on the span. See Chapter 5, "Create Circuits and VT Tunnels" DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 From the View menu on the node view choose **Go to Network View**. If you are already in network view, go to Step 2.

Step 2 Right-click the green line containing the circuits you want to view and choose one of the following:

- **Circuits**—To view BLSR, UPSR, 1+1, or unprotected circuits on the span.
- **PCA Circuits**—To view circuits routed on a BLSR protected channel. This option does not display if the span you right-clicked is not a BLSR span.

On the Circuits on Span dialog box, you can view the following information for circuits provisioned on the span:

- STS—STSs used by the circuits.
- VT—VTs used by the circuits (VT circuits).
- UPSR—(UPSR span only)—If checked, UPSR circuits are on the span.
- Circuit—Displays the circuit name.
- Switch State—(UPSR span only) Displays the switch state of the circuit, that is, whether any span switches are active. For UPSR spans, switch types include: CLEAR (no spans are switched), MANUAL (a Manual switch is active), FORCE (a Force switch is active), and LOCKOUT OF PROTECTION (a span lockout is active).

Note You can perform other procedures from the Circuits on Span dialog box. If the span is in a UPSR, you can switch the span traffic. See "DLP-B197 Initiate a UPSR Force Switch" task on page 13-16 for instructions. If you want to edit a circuit on the span, double-click the circuit. See the "DLP-B231 Edit a Circuit Name" task on page 8-8 or the "DLP-B233 Edit UPSR Circuit Path Selectors" task on page 8-10 for instructions.

Step 3 Return to your originating procedure (NTP).

NTP-B151 Modify Circuit Characteristics

Purpose	This procedure modifies the properties of ONS 15327 circuits.
Tools/Equipment	None
Prerequisite Procedures	Circuits must exist on the network. See Chapter 5, "Create Circuits and VT Tunnels" for circuit creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into the network containing the circuit you want to modify. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. If you are already logged in, continue with Step 2.

Step 2 As needed, complete the "DLP-B231 Edit a Circuit Name" task on page 8-8.

Step 3 As needed, complete the "DLP-B232 Change Active and Standby Span Color" task on page 8-9.

Step 4 As needed, complete the "DLP-B233 Edit UPSR Circuit Path Selectors" task on page 8-10.

Stop. You have completed this procedure.

DLP-B230 Change a Circuit State

Purpose	Use this task to change the state of a circuit.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Click the **Circuits** tab.

Step 2 Click the circuit with the state you want to change.

Note You cannot edit the circuit state if the circuit is routed to nodes with a CTC software release older than Release 3.4. These circuits will automatically be in service (IS).

Step 3 From the Tools menu, choose **Circuits > Set Circuit State**.

Note Alternatively, you can click the **Edit** button, then click the **State** tab on the Edit Circuits window.

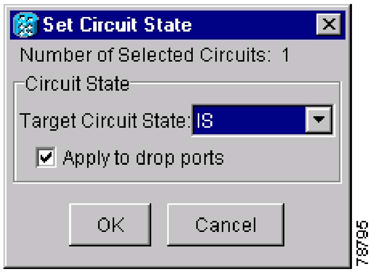
Step 4 In the Set Circuit State dialog box (Figure 8-1) change the circuit state by choosing one of the following choices from the Target Circuit State drop-down menu:

- IS—Places the circuit in service
- OOS—Places the circuit out of service
- OOS-AINS—Places the circuit out of service, auto in service
- OOS-MT—Places the circuit out of service, maintenance

See Table 8-2 on page 8-3 for additional information about circuit states.

Step 5 If you want to apply the state to the circuit source and destination ports, check the **Apply to Drop Ports** check box.

Figure 8-1 Changing Circuit State



Set Circuit State

Number of Selected Circuits: 1

Circuit State

Target Circuit State: IS

☑ Apply to drop ports

Step 6 Click **OK**.

Note CTC will not change the state of the circuit source and destination port in certain circumstances. For example, if the circuit size is smaller than the port, for example, a VT1.5 circuit on an STS port, CTC will not change the port state from IS to OOS. If CTC cannot change the port state, a message is displayed and you will need to change the port state manually.

Step 7 Return to your originating procedure (NTP).

DLP-B231 Edit a Circuit Name

Purpose	Use this task to edit a circuit name.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23

Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Click the **Circuits** tab.

Step 2 Click the circuit you want to rename, then click **Edit**.

Step 3 On the General tab, click the **Name** field and edit or rename the circuit. Names can be up to 48 alphanumeric and/or special characters. However, to ensure that a monitor circuit can be created on this circuit, do not make the name longer than 44 characters because monitor circuits will add "_MON" (four characters) to the circuit name.

Step 4 Click the **Apply** button.

Step 5 From File menu, select **Close**.

Step 6 On the Circuits window, verify that the circuit was correctly renamed.

Step 7 Return to your originating procedure (NTP).

DLP-B232 Change Active and Standby Span Color

Purpose	Use this task to change the color of active (working) and standby (protect) circuit spans on the detailed circuit map of the Edit Circuits window. By default, working spans are green and protect spans are purple.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Edit menu, choose **Preferences**.

Step 2 On the Preferences dialog box, click the **Circuit** tab.

Step 3 Complete one or more of the following steps, as required:

- To change the color of the active (working) span, continue with Step 4.
- To change the color of the standby (protect) span, continue with Step 5.
- To return active and standby spans to their default colors, continue with Step 6.

Step 4 Change the color of the active span:

a. Next to Active Span Color, click the **Color** button.

b. On the Pick a Color dialog box, click the color for the active span, or click the **Reset** button if you want the active span to display the last applied (saved) color.

c. Click **OK** to close the Pick a Color dialog box. If you want to change the standby span color, continue with Step 5. If not, click **OK** to save the change and close the Preferences dialog box, or click **Apply** to save the change and keep the Preferences dialog box displayed.

Step 5 Change the color of the standby span:

a. Next to Standby Span Color, click the **Color** button.

b. On the Pick a Color dialog box, click the color for the standby span, or click the **Reset** button if you want the standby span to display the last applied (saved) color.

c. Click **OK** to save the change and close the Preferences dialog box, or click **Apply** to save the change and keep the Preferences dialog box displayed.

Step 6 Return the active and standby spans to their default colors:

a. From the Edit menu, choose **Preferences**.

b. On the Preferences dialog box, click the **Circuits** tab.

c. Click the **Reset to Defaults** button.

d. Click **OK** to save the change and close the Preferences dialog box, or click **Apply** to save the change and keep the Preferences dialog box displayed.

Step 7 Return to your originating procedure (NTP).

DLP-B233 Edit UPSR Circuit Path Selectors

Purpose	Use this task to change the UPSR signal fail and signal degrade thresholds, the reversion and reversion time, and the PDI-P settings for one or more UPSR circuits.
Tools/Equipment	None
Prerequisite Procedures	NTP-B44 Provision UPSR Nodes, page 4-22 DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Click the **Circuits** tab.

Step 2 Click the UPSR circuit(s) you want to edit. To change the settings for multiple circuits, press the **Shift** key (to choose adjoining circuits) or the **Ctrl** key (to choose non-adjoining circuits) and click each circuit you want to change.

Step 3 From the Tools menu, choose **Circuits > Set Path Selector Attributes**.

Note Alternatively, for single circuits you can click the **Edit** button, then click the **UPSR Selectors** tab on the Edit Circuits window.

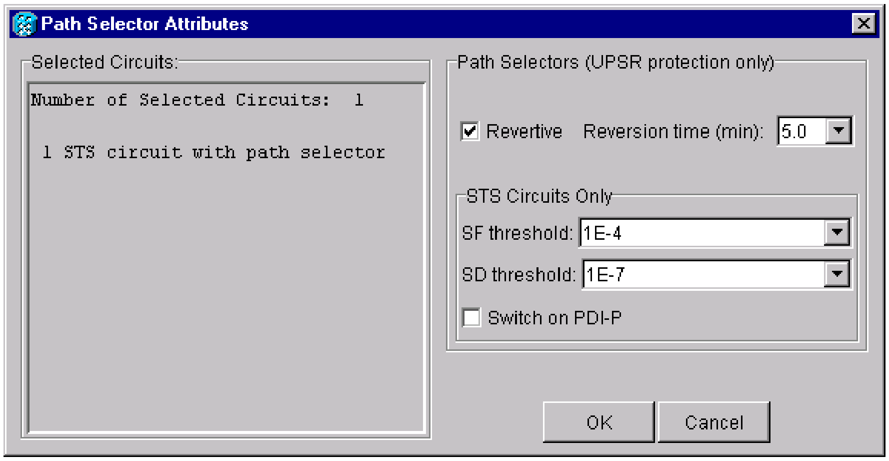
Step 4 In the Path Selectors Attributes dialog box (Figure 8-2), edit the following UPSR selectors, as needed:

- Revertive—If checked, traffic reverts to the working path when conditions that diverted it to the protect path are repaired. If the check box is not selected, traffic does not revert.
- Reversion Time (Min)—If Revertive is checked, this value sets the amount of time that will elapse before traffic reverts to the working path. The range is 0.5 to 12 minutes in 0.5 minute increments.

- SF Ber Level—Sets the UPSR signal failure BER threshold (STS circuits only).
- SD Ber Level—Sets the UPSR signal degrade BER threshold (STS circuits only).
- PDI-P—When checked, traffic switches if an STS payload defect indication is received (STS circuits only).

Step 5 Click **OK** and verify that the changed values are correct.

Figure 8-2 Editing UPSR Path Selectors



Path Selector Attributes

Selected Circuits:

```
Number of Selected Circuits:  1

 1 STS circuit with path selector
```

Path Selectors (UPSR protection only)

☑ Revertive Reversion time (min): 5.0

STS Circuits Only

SF threshold: 1E-4

SD threshold: 1E-7

☐ Switch on PDI-P

78796

Step 6 Return to your originating procedure (NTP).

NTP-B416 Convert a CTC Circuit to TL1 Cross-Connects

Purpose	Use this procedure to convert CTC circuits to a set of TL1 cross-connects, which enables you to repair a missing cross-connect or change the cross-connect(s) using the TL1-like circuit option during circuit creation.
Tools/Equipment	None
Prerequisite Procedures	Circuits must exist on the network. See Chapter 5, “Create Circuits and VT Tunnels” for circuit creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note You can only use this procedure with DS-1, DS-3, or OC-N circuits. You cannot use the procedure with Ethernet circuits, VT tunnels, or VT aggregation points.

Step 1 Log into an ONS 15327 node on the network where you want to convert the CTC circuits. See the “DLP-B60 Log into CTC” task on page 2-23 for instructions. If you are already logged in, continue with Step 2.

Step 2 From the View menu choose **Go to Network View**.

Step 3 Click the **Circuits** tab and choose the CTC circuit(s) that you want to convert to TL1 cross-connects. The circuit(s) must have an INCOMPLETE or ACTIVE status.

Step 4 From the Tools menu, choose **Circuits > Convert CTC Circuit to TL1 Cross-Connects**.

Step 5 In the Convert to TL1 Cross Connect dialog box, click **OK**.

The Convert to TL1 Cross Connect Results dialog box displays the results of the conversion. If any circuits could not be converted, those circuits are listed.

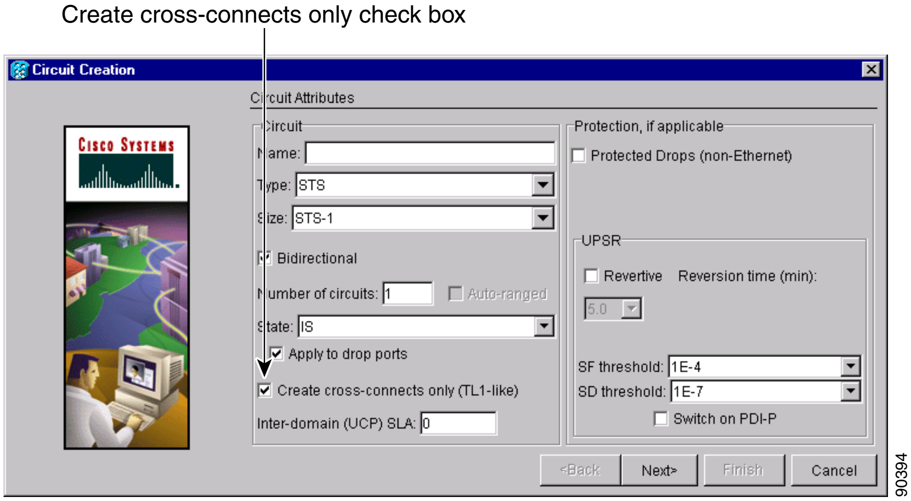
Step 6 In the Convert to TL1 Cross Connect Results dialog box, click **OK**.

If the circuit you selected had an INCOMPLETE status, its status will not change. If you selected an ACTIVE (complete) circuit, its status will change to UPGRADABLE.

Step 7 If you are repairing a circuit, complete the circuit creation procedure in Chapter 5, "Create Circuits and VT Tunnels," appropriate to the circuit you are repairing to replace or repair the circuit cross-connects. On the Circuit Creation wizard, shown in Figure 8-3, check **Create cross-connects only (TL1-like)**.

After you repair or replace all missing cross-connects, CTC automatically merges them and the circuit status changes to UPGRADEABLE.

Figure 8-3 Choosing the Cross-Connects Only Option



Circuit Attributes

Circuit

Name:

Type: STS

Size: STS-1

☑ Bidirectional

Number of circuits: 1 □ Auto-ranged

State: IS

☑ Apply to drop ports

☑ Create cross-connects only (TL1-like)

Inter-domain (UCP) SLA: 0

Protection, if applicable

□ Protected Drops (non-Ethernet)

UPSR

□ Revertive Reversion time (min): 5.0

SF threshold: 1E-4

SD threshold: 1E-7

□ Switch on PDI-P

Step 8 To upgrade the repaired circuit to a CTC circuit, complete the "NTP-B417 Upgrade TL1 Cross-Connects to CTC Circuits" procedure on page 8-13.

Stop. You have completed this procedure.

NTP-B417 Upgrade TL1 Cross-Connects to CTC Circuits

Purpose	Use this procedure to convert a series of cross-connects displayed as UPGRADABLE in the CTC Circuits window to an ACTIVE CTC circuit.
Tools/Equipment	None
Prerequisite Procedures	TL1-created or CTC-created TL1-like cross-connects must exist on the network. See Chapter 5, "Create Circuits and VT Tunnels" for cross-connect creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into an ONS 15327 node on the network where you want to upgrade the TL1-created or CTC-created TL1-like cross-connects. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Circuits** tab and choose one or more circuits with an UPGRADABLE status. These circuits contain a series of cross-connects that are linked together to form a circuit path. The cross-connects might have been created with TL1 or with CTC using the TL1-like cross-connects option.

Step 4 From the Tools menu choose **Circuits > Upgrade TL1 Cross-Connects to CTC Circuits**.

Step 5 On the Upgrade Circuits dialog box, click **OK**.

The circuit status changes to ACTIVE.

Step 6 On the Circuit Upgrade Results dialog box, click **OK**.

Stop. You have completed this procedure.

NTP-B152 Delete Circuits

Purpose	Use this procedure to delete circuits.
Tools/Equipment	None
Prerequisite Procedures	Circuits must exist on the network. See Chapter 5, "Create Circuits and VT Tunnels" for circuit creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into an ONS 15327 node on the network where you want to delete the circuit. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

Step 3 Investigate all network alarms and resolve any problems that may be affected by the circuit deletion. Refer to the Alarm Troubleshooting chapter in the *Cisco ONS 15327 Troubleshooting Guide*.

Step 4 Verify that traffic is no longer carried on the circuit, using local site practices, and that the circuit can be safely deleted.

Step 5 Click the **Circuits** tab.

Step 6 Choose the circuit(s) you want to delete, then click **Delete**.

Step 7 On the Delete Circuits confirmation dialog box, check **Set drop ports to OOS** if you want to put the circuit source and destination ports out of service. (CTC will place the ports out of service only if the circuit is the same size as the port or is the only circuit using the port.) Click **Yes** to confirm the deletion.

Step 8 Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

Stop. You have completed this procedure.

NTP-B78 Create a Monitor Circuit

Purpose	Use this procedure to create a monitor circuit that monitors traffic on primary, bidirectional circuits.
Tools/Equipment	None
Prerequisite Procedures	Bidirectional (2-way) circuits must exist on the network. See Chapter 5, "Create Circuits and VT Tunnels" for circuit creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Monitor circuits cannot be used with EtherSwitch circuits.

Note For unidirectional circuits, create a drop to the port where the test equipment is attached.

Step 1 Log into an ONS 15327 node on the network where you will create the monitor circuit. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. If you are already logged in, continue with Step 2.

Step 2 From the View menu choose **Go to Network View**.

Step 3 Click the **Circuits** tab.

Step 4 Choose the bidirectional (2-way) circuit that you want to monitor and double-click it (or click **Edit**).

Step 5 Verify that the circuit name is no more than 44 characters. Monitor circuits append a "_MON" to the circuit name. If the name is longer than 44 characters, edit the name in the Name field, then click **Apply**.

Step 6 On the Edit Circuit window, click the **Monitors** tab.

The Monitors tab displays ports that you can use to monitor the circuit.

Note The Monitor tab is only available when the circuit has an ACTIVE status.

Step 7 On the Monitors tab, choose the monitor source port. The monitor circuit will display traffic coming into the node at the port you choose.

Step 8 Click **Create Monitor Circuit**.

Step 9 In the Circuit Destination section of the Circuit Creation wizard, choose the destination node, slot, port, STS, VT, or DS1 for the monitored circuit.

Step 10 Click **Next**.

Step 11 On the Circuit Routing Preferences panel, review the monitor circuit information. If you want the monitor circuit routed on a BLSR protection channel, click **Protection Channel Access**.

Step 12 Click **Finish**.

Step 13 On the Edit Circuit window, click **Close**. The new monitor circuit appears on the Circuits tab.

Stop. You have completed this procedure.

NTP-B79 Create a J1 Path Trace

Purpose	Use this procedure to create a repeated, fixed-length string of characters used to monitor interruptions or changes to circuit traffic.
Tools/Equipment	ONS 15327 cards capable of transmitting and/or receiving path trace must be installed. See Table 8-3 on page 8-16 for a list of cards.
Prerequisite Procedures	Path trace can only be provisioned on OC-N (STS) circuits. See Chapter 5, "Create Circuits and VT Tunnels" for OC-N circuit creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into the node on the network where you will create the path trace. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. If you are already logged in, continue with Step 2.

Step 2 Complete the following tasks as needed:

- DLP-B264 Provision Path Trace on Circuit Source and Destination Ports, page 8-16
- DLP-B137 Provision Path Trace on OC-N Ports, page 8-19

Stop. You have completed this procedure.

DLP-B264 Provision Path Trace on Circuit Source and Destination Ports

Purpose	Use this task to create a path trace on STS circuit source ports and destination ports.
Tools/Equipment	ONS 15327 cards capable of transmitting and receiving path trace must be installed at the circuit source and destination ports. See Table 8-3 on page 8-16 for a list of cards.
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This procedure assumes you are setting up path trace on a bidirectional circuit and setting up transmit strings at the circuit source and destination.

Step 1 Click the **Circuits** tab.

Step 2 For the STS circuit you want to monitor, verify that the source and destination ports are on a card that can transmit and receive the path trace string. See Table 8-3 for a list of cards.

Table 8-3 ONS 15327 Cards Capable of Path Trace

J1 Function	Cards
Transmit and Receive	XTC (DS-1) G1000-2
Receive Only	OC3 IR 4 1310 OC12 IR 1310, OC12 LR 1550 OC48 IR 1310, OC48 LR 1550

If neither port is on a transmit/receive card, you will not be able to complete this task. If one port is on a transmit/receive card and the other is on a receive-only card, you can set up the transmit string at the transmit/receive port and the receive string at the receive-only port, but you will not be able to transmit in both directions.

Step 3 Choose the STS circuit you want to trace, then double-click it (or click **Edit**).

Step 4 On the Edit Circuit window, click the **Show Detailed Map** check box at the bottom of the window. A detailed map of the source and destination ports is displayed.

Step 5 Provision the circuit source transmit string:

a. On the detailed circuit map right-click the circuit source port (the square on the left or right of the source node icon) and choose **Edit J1 Path Trace (port)** from the shortcut menu.

b. In the New Transmit String field, enter the circuit source transmit string. Enter a string that makes the source port easy to identify, such as the node IP address, node name, circuit name, or another string. If the New Transmit String field is left blank, the J1 transmits a string of null characters.

c. Click **Apply**, then click **Close.**

Step 6 Provision the circuit destination transmit string:

a. On the detailed circuit map, right-click the circuit destination port and choose **Edit Path Trace** from the shortcut menu.

b. In the New Transmit String field, enter the string that you want the circuit destination to transmit. Enter a string that makes the destination port easy to identify, such as the node IP address, node name, circuit name, or another string. If the New Transmit String field is left blank, the J1 transmits a string of null characters.

c. Click **Apply.**

Step 7 Provision the circuit destination expected string:

a. In the Circuit Path Trace window, enable the path trace expected string by choosing **Auto** or **Manual** from the Path Trace Mode drop-down menu:

- Auto—The first string received from the source port is the baseline. An alarm is raised when a string that differs from the baseline is received.
- Manual—The string entered in the Current Expected String is the baseline. An alarm is raised when a string that differs from the Current Expected String is received.

b. If you set the Path Trace Mode field to Manual, enter the string that the circuit destination should receive from the circuit source in the New Expected String field. If you set the Path Trace Mode field to Auto, skip this step.

c. Click the **Disable AIS if TIM-P is detected** check box if you want to suppress the alarm indication signal (AIS) when the STS Path Trace Identifier Mismatch Path (TIM-P) alarm is displayed. Refer to the *Cisco ONS 15327 Troubleshooting Guide* for descriptions of alarms and conditions.

Note Remote Defect Indicator (RDI) conditions on TIM-P are not generated in this software release.

d. Click **Apply**, then click **Close.**

Step 8 Provision the circuit source expected string:

a. On the Edit Circuit window (with Show Detailed Map chosen) right-click the circuit source port and choose **Edit Path Trace** from the shortcut menu.

b. In the Circuit Path Trace window, enable the path trace expected string by choosing **Auto** or **Manual** from the Path Trace Mode drop-down menu:

- Auto—Uses the first string received from the port at the other end as the baseline string. An alarm is raised when a string that differs from the baseline is received.
- Manual—Uses the Current Expected String field as the baseline string. An alarm is raised when a string that differs from the Current Expected String is received.

c. If you set Path Trace Mode to Manual, enter the string that the circuit source should receive from the circuit destination in the New Expected String field. If you set Path Trace Mode to Auto, skip this step.

d. Click the **Disable AIS and RDI if TIM-P is detected** check box if you want to suppress the alarm indication signal (AIS) when the STS Path Trace Identifier Mismatch Path (TIM-P) alarm is displayed. Refer to the *Cisco ONS 15327 Troubleshooting Guide* for descriptions of alarms and conditions.

Note Remote Defect Indicator (RDI) conditions on TIM-P are not generated in this software release.

e. Click **Apply.**

Step 9 After you set up the path trace, the received string appears in the Received field on the path trace setup window. Figure 8-4 shows an example. The following options are available:

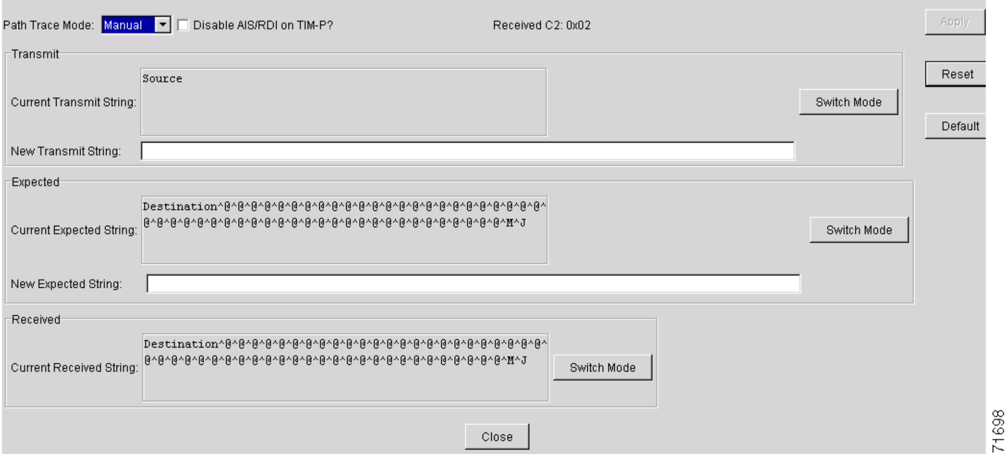
- Click **Hex Mode** to display path trace in hexadecimal display. The button name changes to ASCII Mode. Click it to return the path trace to ASCII display.
- Click the **Reset** button to reread values from the port.
- Click **Default** to return to the path trace default settings (Path Trace Mode is set to Off and the New Transmit and New Expected Strings are null).

Caution Clicking Default will generate alarms if the port on the other end is provisioned with a different string.

The Expect and Receive strings are updated every few seconds if the Path Trace Mode field is set to Auto or Manual.

Step 10 Click **Close.**

Figure 8-4 Setting Up a Path Trace



Path Trace Mode: Manual

□ Disable AIS/RDI on TIM-P?

Received C2: 0x02

Transmit

Current Transmit String: Source

New Transmit String:

Expected

Current Expected String:

```
Destination^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^M^J
```

New Expected String:

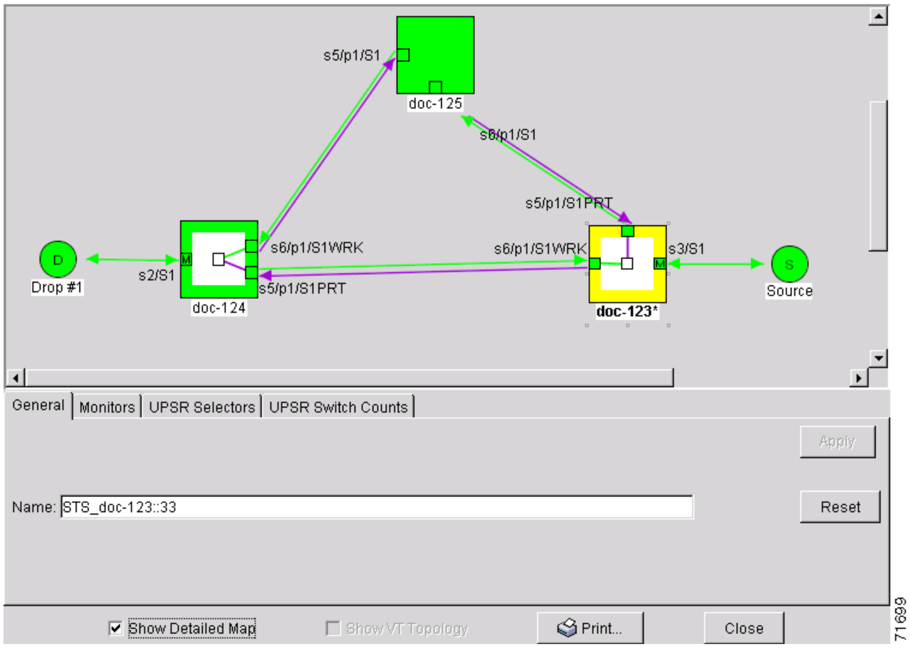
Received

Current Received String:

```
Destination^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^M^J
```

When you display the detailed circuit window, path trace is indicated by an M (manual path trace) or an A (automatic path trace) at the circuit source and destination ports. Figure 8-5 shows an example.

Figure 8-5 Detailed Circuit Window With Manual Expected String Enabled



Name: STS_doc-123::33

Step 11 Return to your originating procedure (NTP).

DLP-B137 Provision Path Trace on OC-N Ports

Purpose	Use this task to monitor a path trace on OC-N ports within the circuit path.
Tools/Equipment	The OC-N ports you want to monitor must be on OC-N cards capable of receiving path trace. See Table 8-3 on page 8-16.
Prerequisite Procedures	DLP-B264 Provision Path Trace on Circuit Source and Destination Ports, page 8-16 DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Display the node where path trace was provisioned on the circuit source and destination ports.

Step 2 Click **Circuits**.

Step 3 Choose the STS circuit that has path trace provisioned on the source and destination ports, then click **Edit**.

Step 4 On the Edit Circuit window, click the Show Detailed Map check box at the bottom of the window. A detailed circuit graphic showing source and destination ports appears.

Step 5 In the detailed circuit map right-click the circuit OC-N port (the square on the left or right of the source node icon) and choose **Edit Path Trace** from the shortcut menu.

Note The OC-N port must be on a receive-only card listed in Table 8-3 on page 8-16. If not, the Edit Path Trace menu item will not appear.

Step 6 In the Circuit Path Trace window, enable the path trace expected string by choosing **Auto** or **Manual** from the Path Trace Mode drop-down menu:

- Auto—Uses the first string received from the port at the other end as the baseline string. An alarm is raised when a string that differs from the baseline is received. For OC-N ports, Auto is recommended, since Manual mode requires you to trace the circuit on the Edit Circuit window to determine whether the port is the source or destination path.
- Manual—Uses the Current Expected String field as the baseline string. An alarm is raised when a string that differs from the Current Expected String is received.

Step 7 If you set the Path Trace Mode field to Manual, enter the string that the OC-N port should receive in the New Expected String field. To do this, trace the circuit path on the detailed circuit window to determine whether the port is in the circuit source or destination path, then set the New Expected String field to the string transmitted by the circuit source or destination. If you set the Path Trace Mode field to Auto, skip this step.

Step 8 Click **Apply**, then click **Close.**

Step 9 Return to your originating procedure (NTP).

CHAPTER 9

Change Port Settings

This chapter explains how to change transmission settings on electrical and optical ports in a Cisco ONS 15327.

Before You Begin

Before performing any of the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15327 Troubleshooting Guide* as necessary.

Caution Changing card or port settings can be service affecting. You should make all changes during a scheduled maintenance window.

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-B88 Modify Line Settings and PM Parameter Thresholds for Electrical Ports, page 9-1—Complete as needed.
2. NTP-B89 Modify Line Settings and PM Parameter Thresholds for Optical Ports, page 9-9—Complete as needed.

NTP-B88 Modify Line Settings and PM Parameter Thresholds for Electrical Ports

Purpose	This procedure changes the line and threshold settings for electrical ports; default values are listed in the "Card Default Settings" section on page C-4.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at the node where you want to change the card/port settings.

Step 2 Complete the "NTP-B108 Back Up the Database" procedure on page 14-6 to preserve the existing database.

Step 3 Perform either of the following tasks as needed:

- DLP-B165 Change Line and Threshold Settings for the DS-1 Ports, page 9-2
- DLP-B166 Change Line and Threshold Settings for the DS-3 Ports, page 9-6

Step 4 When you are finished changing the port settings, complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

Stop. You have completed this procedure.

DLP-B165 Change Line and Threshold Settings for the DS-1 Ports

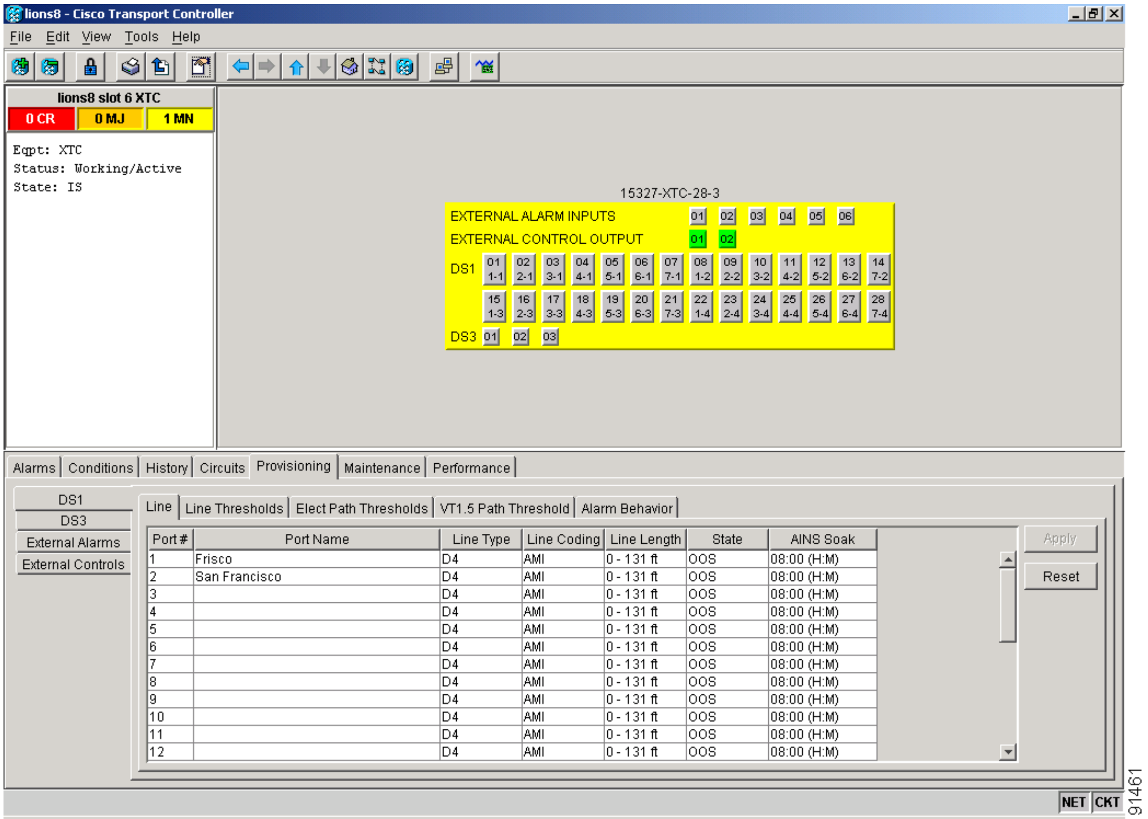
Purpose	This task changes the line and threshold settings for the DS-1 ports. The default DS-1 port settings are listed in Table C-1 on page C-5.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The ONS 15327 XTC cards provide 14 (XTC-14) or 28 (XTC-28-3) DS-1 ports. Each port operates at 1.544 Mbps. Default thresholds are based on recommendations in GR-820-CORE, Section 4.0.

Step 1 In node view, double-click the XTC card where you want to change the DS-1 line or threshold settings.

Step 2 Click the **Provisioning** > DS-1 tabs (Figure 9-1).

Figure 9-1 Provisioning Line Parameters on the DS-1 Ports


lions8 - Cisco Transport Controller
File Edit View Tools Help
lions8 slot 6 XTC
0 CR
0 MJ
1 MN
15327-XTC-28-3
EXTERNAL ALARM INPUTS 01 02 03 04 05 06
EXTERNAL CONTROL OUTPUT 01 02
DS1 01 1-1 02 2-1 03 3-1 04 4-1 05 5-1 06 6-1 07 7-1 08 1-2 09 2-2 10 3-2 11 4-2 12 5-2 13 6-2 14 7-2
15 1-3 16 2-3 17 3-3 18 4-3 19 5-3 20 6-3 21 7-3 22 1-4 23 2-4 24 3-4 25 4-4 26 5-4 27 6-4 28 7-4
DS3 01 02 03
Alarms Conditions History Circuits Provisioning Maintenance Performance
DS1
DS3
External Alarms
External Controls
Line Line Thresholds Elect Path Thresholds VT1.5 Path Threshold Alarm Behavior
Apply
Reset
NET CKT
91461

Eqpt: XTC
Status: Working/Active
State: IS

Port #	Port Name	Line Type	Line Coding	Line Length	State	AINS Soak
1	Frisco	D4	AMI	0 - 131 ft	OOS	08:00 (H:M)
2	San Francisco	D4	AMI	0 - 131 ft	OOS	08:00 (H:M)
3		D4	AMI	0 - 131 ft	OOS	08:00 (H:M)
4		D4	AMI	0 - 131 ft	OOS	08:00 (H:M)
5		D4	AMI	0 - 131 ft	OOS	08:00 (H:M)
6		D4	AMI	0 - 131 ft	OOS	08:00 (H:M)
7		D4	AMI	0 - 131 ft	OOS	08:00 (H:M)
8		D4	AMI	0 - 131 ft	OOS	08:00 (H:M)
9		D4	AMI	0 - 131 ft	OOS	08:00 (H:M)
10		D4	AMI	0 - 131 ft	OOS	08:00 (H:M)
11		D4	AMI	0 - 131 ft	OOS	08:00 (H:M)
12		D4	AMI	0 - 131 ft	OOS	08:00 (H:M)

Step 3 Depending on the setting you need to modify, click the **Line**, **Line Thresholds**, **Elect Path Thresholds**, **VT1.5 Path Threshold,** or **Alarm Behavior** subtab.

Note See Chapter 6, "Manage Alarms" for information about the Alarm Behavior subtab.

Step 4 Modify any of the settings found under these subtabs.

For definitions of the line settings, see Table 9-1. For definitions of the line threshold settings, see Table 9-2 on page 9-4. For definitions of the electrical path settings, see Table 9-3 on page 9-5.

For the factory default settings for the DS-1 ports, see Table C-1 on page C-5.

Step 5 Click **Apply**.

Step 6 Repeat Steps 4 and 5 for each subtab that has parameters you want to provision.

Table 9-1 describes the values on the Provisioning > Line subtab for the DS-1 ports.

Table 9-1 Line Options for DS-1 Ports

Parameter	Description	Options
Port #	Port number	• 1 to 14 (XTC-14) • 1 to 28 (XTC-28-3)
Port	Port name	User-defined, up to 32 alphanumeric/special characters. Blank by default See DLP-B314 Assign a Name to a Port, page 5-14.
Line Type	Defines the line framing type	• D4 • ESF - Extended Super Frame • Unframed
Line Coding	Defines the DS-1 transmission coding type	• AMI - Alternate Mark Inversion (default) • B8ZS - Bipolar 8 Zero Substitution
Line Length	Defines the distance (in feet) from backplane connection to the next termination point	• 0 - 131 (default) • 132 - 262 • 263 - 393 • 394 - 524 • 525 - 655
State	Places port in service, out of service, out of service-maintenance, or out of service-auto in service.	• IS • OOS • OOS_MT • OOS_AINS
AINS Soak	Automatic in-service soak	• Duration of valid input signal in hh.mm after which the port is set in service by the software. • 0 to 48 hours, 15 minutes increments.

Table 9-2 describes the values on the Provisioning > Line Thresholds subtab for the DS-1 ports.

Table 9-2 Line Thresholds Options for DS-1 Ports

Parameter	Description	Options
Port	Port number	• 1 to 14 (XTC-14) • 1 to 28 (XTC-28-3)
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button.
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button.

Table 9-2 Line Thresholds Options for DS-1 Ports (continued)

Parameter	Description	Options
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button.
LOSS	Number of one-second intervals containing one or more loss of signal (LOS) defects	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button.

Table 9-3 on page 9-5 describes the values on the Provisioning > Elect Path Thresholds subtab for the DS-1 ports.

Table 9-3 Electrical Path Threshold Options for DS-1 Ports

Parameter	Description	Options
Port	Port number	• 1 to 14 (XTC-14) • 1 to 28 (XTC-28-3)
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button.
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button.
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button.
SAS	Severely errored frame/alarm indication signal	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button.
AISS	Alarm indication signal seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button.
UAS	Unavailable seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button.

Table 9-4 describes the values on the Provisioning > VT1.5 Path Thresholds subtab for the DS-1 ports.

Table 9-4 VT1.5 Path Thresholds Options for DS-1 ports

Parameter	Description	Options
Port #	DS-1 ports partitioned for STS	Read-only Line 1, STS 1, Line 2, STS 1 Line 3, STS 1, Line 4 STS 1
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button (Near End, STS termination).
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button (Near End, STS termination).
FC	Failure count	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button (Near End, STS termination).
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button (Near End, STS termination).
UAS	Unavailable seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button (Near End, STS termination).

Note The threshold value displays after the circuit is created.

Step 7 Return to your originating procedure (NTP).

DLP-B166 Change Line and Threshold Settings for the DS-3 Ports

Purpose	This task changes the line and threshold settings for the DS-3 ports. The default DS-3 values are listed in Table C-2 on page C-7.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, double-click the XTC-28-3 card where you want to change the DS-3 line or threshold settings.

Step 2 Click the **Provisioning** tab.

Step 3 Click the **DS-3** tab.

Step 4 Depending on the setting you need to modify, click the **Line**, **Line Thresholds**, **STS-1 Path Threshold**, or **Alarm Behavior** subtab.

Note See Chapter 6, "Manage Alarms" for information about the Alarm Behavior subtab.

Step 5 Modify any of the settings found under these subtabs. For definitions of the Line settings, see Table 9-5 on page 9-7. For definitions of the Line Threshold settings, see Table 9-6 on page 9-8. For definitions of the SONET Threshold settings, see Table 9-7 on page 9-8.

For the factory default settings for the DS-3 ports, see Table C-2 on page C-7.

Step 6 Click **Apply**.

Step 7 Repeat Steps 5 and 6 for each subtab that has parameters you want to provision.

Table 9-5 describes the values on the Provisioning > Line subtab for the DS-3 ports.

Table 9-5 Line Options for DS-3 Ports

Parameter	Description	Options
Port #	Port number	1 to 3
Port	Port name	User-defined, up to 32 alphanumeric/ special characters. Blank by default. See DLP-B314 Assign a Name to a Port, page 5-14.
Line Length	Defines the distance (in feet) from backplane connection to the next termination point	• 0 - 225 (default) • 226 - 450
State	Places port in service, out of service, out of service-maintenance, or out of service-auto in service.	• IS • OOS • OOS_MT • OOS_AINS
AINS Soak	Automatic in-service soak	Time of presence of valid input signal in hh.mm after which the port is set in service by the software. 0 to 48 hours, 15 minutes increments.

Table 9-6 describes the values on the Provisioning > Line Thresholds subtab for the DS-3 ports.

Table 9-6 Line Threshold Options for DS-3 Ports

Parameter	Description	Options
Port #	Port number	1 to 3
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button.
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button.
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button.
LOSS	Loss of signal; number of one-second intervals containing one or more LOS defects	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button.

Table 9-7 describes the values on the Provisioning > STS-1 Path Threshold subtab for the DS-3 ports.

Table 9-7 STS-1 Path Threshold Options for DS-3 Ports

Parameter	Description	Options
Port #	DS-3 ports partitioned for STS	Read-only DS-3 ports 1 to 3 any available STS
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button (Near and Far End, STS termination only).
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button (Near and Far End, STS termination only).
FC	Failure count	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button (Near and Far End, STS termination only).
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button (Near and Far End, STS termination only).
UAS	Unavailable seconds	Numeric. Can be set for 15-minute or one-day intervals. Select the bullet and click the Refresh button (Near and Far End, STS termination only).

Note The threshold value displays after the circuit is created.

Step 8 Return to your originating procedure (NTP).

NTP-B89 Modify Line Settings and PM Parameter Thresholds for Optical Ports

Purpose	This procedure changes the line and threshold settings for optical cards and ports. The default OC-N card settings are provided in the "Card Default Settings" section on page C-4.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23 at the node where you want to change the card settings. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

Step 3 Perform any of the following tasks as needed:

- DLP-B170 Change Line Settings for OC-N Cards, page 9-9
- DLP-B171 Change SONET Thresholds Settings for OC-N Cards, page 9-11
- DLP-B172 Change an Optical Port to SDH, page 9-14

Step 4 Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

Stop. You have completed this procedure.

DLP-B170 Change Line Settings for OC-N Cards

Purpose	This task changes the line settings for OC-N cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Double-click the OC-N card where you want to change the line settings.

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

Step 3 Modify any of the settings listed in Table 9-8.

See Table C-3 on page C-8 for OC-3 card default settings, Table C-4 on page C-10 for OC-12 card default settings, or Table C-5 on page C-12 for OC-48 card default settings.

Note The STS subtab is used to provision intermediate path performance monitoring (IPPM). To provision IPPM, circuits must be provisioned on the card.

Table 9-8 OC-N Card Line Settings

Parameter	Description	Options
Port #	Port number (read-only)	• 1 to 4 (OC-3) • 1 (OC-12, OC-48)
Port Name	Provides the ability to assign the specified port a name	User-defined, up to 32 alphanumeric/ special characters. Blank by default. See DLP-B314 Assign a Name to a Port, page 5-14.
SF BER	Sets the signal fail bit error rate	• 1E-3 • 1E-4 (default) • 1E-5
SD BER	Sets the signal degrade bit error rate	• 1E-5 • 1E-6 • 1E-7 (default) • 1E-8 • 1E-9
Provides Synch	If checked, the card is provisioned as a network element timing reference	• Yes (checked) • No (unchecked) (Read-only)
EnableSync Msg	Enables synchronization status messages (S1 byte), which allow the node to choose the best timing source	• Yes (checked, default) • No (unchecked)
Send DoNotUse	When checked, sends a DUS (do not use) message on the S1 byte	• Yes (checked) • No (unchecked, default)
PJSTSMon #	Sets the STS that will be used for pointer justification. If set to 0, no STS is monitored. Only one STS can be monitored on each OC-N port.	• 0 - 3 (OC-3, per port) • 0 - 12 (OC-12) • 0 - 48 (OC-48)

Table 9-8 OC-N Card Line Settings (continued)

Parameter	Description	Options
State	Places port in service, out of service, out of service-maintenance, or out of service-auto in service.	• IS • OOS • OOS_MT • OOS_AINS
AINS Soak	Automatic in-service soak	• Duration of valid input signal in hh.mm after which the card is set in service by the software. • 0 to 48 hours, 15 minutes increments.
Type	Defines the port as SONET or SDH. The Enable Sync Msg field and the Send Do Not Use field must be disabled before the port can be set to SDH.	• Sonet • SDH

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

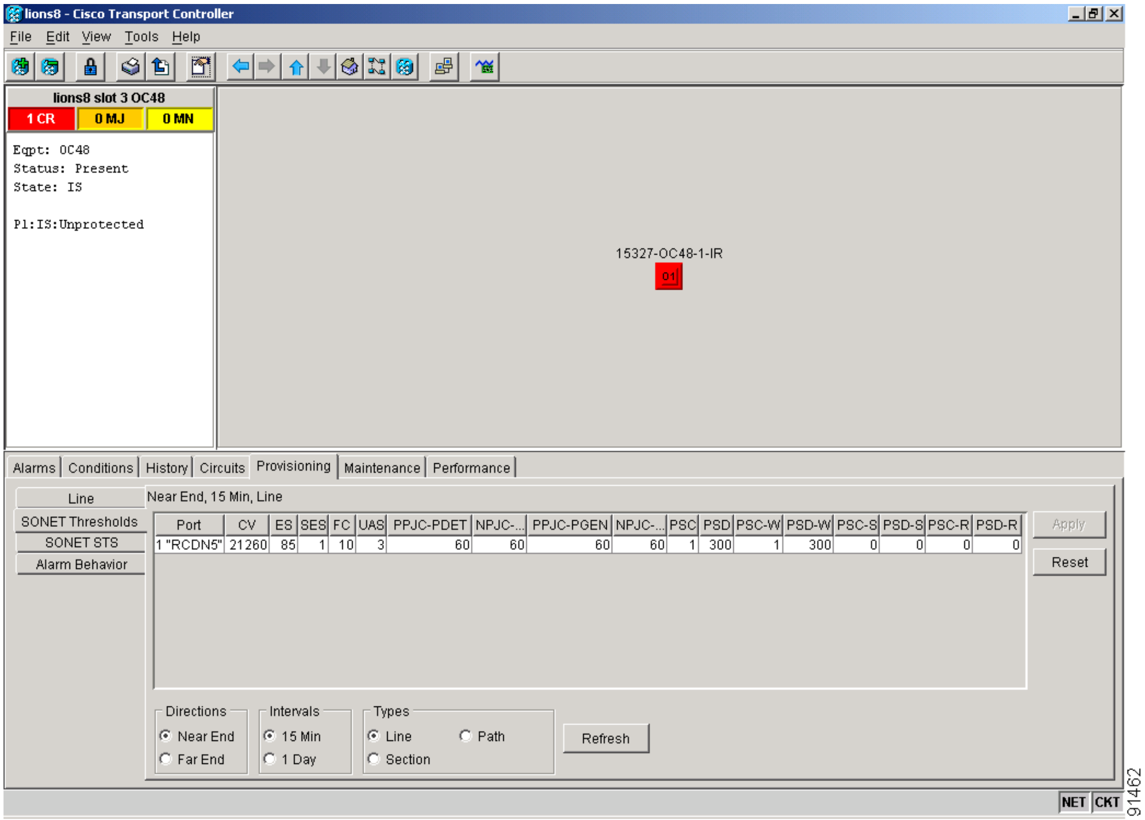
DLP-B171 Change SONET Thresholds Settings for OC-N Cards

Purpose	This task changes SONET thresholds settings for OC-N cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the OC-N card where you want to change the SONET thresholds settings (Figure 9-2).

Step 2 Click the **Provisioning > SONET Thresholds** tabs (Figure 9-2).

Figure 9-2 Provisioning SONET Thresholds for the OC48 IR 1310 Card



```
Eqpt: OC48
Status: Present
State: IS

P1:IS:Unprotected
```

Near End, 15 Min, Line

Port	CV	ES	SES	FC	UAS	PPJC-PDET	NPJC-...	PPJC-PGEN	NPJC-...	PSC	PSD	PSC-W	PSD-W	PSC-S	PSD-S	PSC-R	PSD-R
1 "RCDN5"	21260	85	1	10	3	60	60	60	60	1	300	1	300	0	0	0	0

Directions: ● Near End ○ Far End

Intervals: ● 15 Min ○ 1 Day

Types: ● Line ○ Path ○ Section

Step 3 Modify any of the settings listed in Table 9-9.

See Table C-3 on page C-8 for OC-3 card default settings, Table C-4 on page C-10 for OC-12 card default settings, or Table C-5 on page C-12 for OC-48 card default settings.

Table 9-9 OC-N SONET Thresholds Options

Parameter	Description	Options
Port	Port number	• 1 to 4 (OC-3) • 1 (OC-12, OC-48)
CV	Coding violations	Numeric. Can be set for 15-minute or one-day intervals for Line, Section, or Path (Near and Far End). Select the bullet and click the Refresh button.
ES	Errored seconds	Numeric. Can be set for 15-minute or one-day intervals for Line, Section, or Path (Near and Far End). Select the bullet and click the Refresh button.
SES	Severely errored seconds	Numeric. Can be set for 15-minute or one-day intervals for Line, Section, or Path (Near and Far End). Select the bullet and click the Refresh button.

Table 9-9 OC-N SONET Thresholds Options (continued)

Parameter	Description	Options
SEFS	Severely errored framing seconds	Numeric. Can be set for 15-minute or one-day intervals for Line, Section, or Path (Near and Far End). Select the bullet and click the Refresh button.
FC	Failure count	Numeric. Can be set for 15-minute or one-day intervals for Line. Select the bullet and click the Refresh button. or Path (Near and Far End)
UAS	Unavailable seconds	Numeric. Can be set for 15-minute or one-day intervals for Line or Path (Near and Far End). Select the bullet and click the Refresh button.
PPJC-PDET	Positive Pointer Justification Count, STS Path detected.	Numeric. Can be set for 15-minute or one-day intervals for Line (Near and Far End). Select the bullet and click the Refresh button.
NPJC-PDET	Negative Pointer Justification Count, STS Path detected.	Numeric. Can be set for 15-minute or one-day intervals for Line (Near and Far End). Select the bullet and click the Refresh button.
PPJC-PGEN	Positive Pointer Justification Count, STS Path generated.	Numeric. Can be set for 15-minute or one-day intervals for Line (Near and Far End). Select the bullet and click the Refresh button.
NPJC-PGEN	Negative Pointer Justification Count, STS Path generated.	Numeric. Can be set for 15-minute or one-day intervals for Line (Near and Far End). Select the bullet and click the Refresh button.
PSC	Protection Switching Count (Line)	Numeric. Can be set for 15-minute or one-day intervals for Line (Near and Far End). Select the bullet and click the Refresh button.
PSD	Protection Switch Duration (Line)	Numeric. Can be set for 15-minute or one-day intervals for Line (Near and Far End). Select the bullet and click the Refresh button.
PSC-W	Protection Switching Count - Working line BLSR is not supported on the OC-3 card; therefore, the PSC-W, PSC-S, and PSC-R PMs do not increment.	Numeric. Can be set for 15-minute or one-day intervals for Line (Near and Far End). Select the bullet and click the Refresh button.
PSD-W	Protection Switching Duration - Working line BLSR is not supported on the OC-3 card; therefore, the PSD-W, PSD-S, and PSD-R PMs do not increment.	Numeric. Can be set for 15-minute or one-day intervals for Line (Near and Far End). Select the bullet and click the Refresh button.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-B172 Change an Optical Port to SDH

Purpose	Use this task to provision a port on an OC-N card for SDH.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Double-click the OC-N card where you want to provision a port for SDH.
Before you can change the port type to SDH, ensure the following:

- The EnableSyncMsg and SendDoNotUse fields are unchecked.
- The card is not part of a BLSR or 1+1 protection group.
- The card is not part of an orderwire channel.
- The card is not a SONET DCC termination point.

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

Step 3 In the Type field, specify the port and choose SDH.

Step 4 Click **Apply**.

Step 5 If the card is a multiport OC-N card, such as an OC-3, you can repeat Steps 3 and 4 for any other ports on the card.

Step 6 Return to your originating procedure (NTP).

CHAPTER 10

Change Node Settings

This chapter explains how to modify node provisioning for the Cisco ONS 15327. To provision a new node, see Chapter 3, "Turn Up Node." To change default card-level and node-level settings, see Appendix C, "Network Element Defaults."

Before You Begin

Before performing the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15327 Troubleshooting Guide* as necessary.

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-B81 Change Node Management Information, page 10-2—As needed, complete this procedure to change node name, contact information, latitude, longitude, date, time, and the login legal disclaimer.
2. NTP-B201 Change CTC Network Access, page 10-4—As needed, complete this procedure to change the IP address, default router, subnet mask, network configuration settings, and static routes.
3. NTP-B202 Customize the CTC Network View, page 10-7—As needed, complete this procedure to customize the appearance of the network map, including specifying a different default map, selecting your own map or image, and changing the background color.
4. NTP-B203 Modify or Delete 1+1 Card Protection Settings, page 10-12—Complete as needed.
5. NTP-B85 Change Node Timing, page 10-15—Complete as needed.
6. NTP-B205 Modify Users and Change Security, page 10-17—Complete as needed.
7. NTP-B87 Change SNMP Settings, page 10-23—Complete as needed.

NTP-B81 Change Node Management Information

Purpose	This procedure changes basic information about the node such as node name, date, time, contact information, and the login legal disclaimer.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

Step 3 Click the **Provisioning > General** tabs.

Step 4 Complete the "DLP-B140 Change the Node Name, Date, Time, and Contact Information" task on page 10-2, as needed.

Step 5 Complete the "DLP-B265 Change the Login Legal Disclaimer" task on page 10-3, as needed.

Step 6 After confirming the changes, complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

Stop. You have completed this procedure.

DLP-B140 Change the Node Name, Date, Time, and Contact Information

Purpose	This procedure changes basic information such as node name, date, time, and contact information.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Changing the date, time, or time zone may invalidate the node's performance monitoring counters.

Step 1 In node view, click the **Provisioning > General** tabs.

Step 2 Change any of the following:

- General: Node Name
- General: Contact
- Location: Latitude
- Location: Longitude

- Location: Description

Note To see changes to longitude or latitude on the network map, you must go to network view and right-click the specified node, then click **Reset Node Position**.

- Time: Use SNTP Server
- Time: Date (M/D/Y)
- Time: Time (H:M:S)
- Time: Time Zone
- Time: Use Daylight Saving Time

See the "NTP-B25 Set Up Name, Date, Time, and Contact Information" procedure on page 3-5 for detailed field descriptions.

Step 3 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

Step 4 Return to your originating procedure (NTP).

DLP-B265 Change the Login Legal Disclaimer

Purpose	Use this task to modify the legal disclaimer statement shown in the CTC login dialog box so that it will display customer-specific information when users log into the network.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning > Security > Legal Disclaimer > HTML** tabs.

Step 2 The existing statement is a default, non-customer-specific disclaimer. If you want to edit this statement with specifics for your company, you can change the text. You can also use the following HTML commands to format the text:

- <b> Begins boldface font
- </b> Ends boldface font
- <center> Aligns type in the center of the window
- </center> Ends the center alignment
- <font=n, where n = point size> Changes the font to the new size
- </font> Ends the font size command
- <p> Creates a line break
- <sub> Begins subscript
- </sub> Ends subscript

- <sup> Begins superscript
- </sup> Ends superscript
- <u> Starts underline
- </u> Ends underline

Step 3 If you want to preview your changed statement and formatting, click the **Preview** subtab.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

NTP-B201 Change CTC Network Access

Purpose	This procedure changes essential network information, including IP settings, static routes, and OSPF options.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Additional ONS 15327 networking information and procedures, including IP addressing examples, static route scenarios, Open Shortest Path First (OSPF) protocol, and routing information protocol options are provided in the IP Networking section of the *Cisco ONS 15327 Reference Manual*.

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

Step 3 Perform any of the following tasks as needed:

- DLP-B266 Change IP Settings, page 10-5
- DLP-B142 Modify a Static Route, page 10-6
- DLP-B143 Delete a Static Route, page 10-6
- DLP-B144 Disable the Open Shortest Path First Protocol, page 10-7
- DLP-B250 Set Up or Change Open Shortest Path First Protocol, page 3-10.

Step 4 Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

Stop. You have completed this procedure.

DLP-B266 Change IP Settings

Purpose	This task changes the IP address, subnet mask, default router, DHCP access, firewall access, and proxy server settings for the ONS 15327.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning** > **Network > General** tabs.

Step 2 Change any of the following:

- IP Address
- Default Router
- Subnet Mask Length
- Forward DHCP Request To
- TCC CORBA (IIOP) Listener Port
- Gateway Settings

See the "NTP-B169 Set Up CTC Network Access" procedure on page 3-7 for detailed field descriptions.

Step 3 Click **Apply**.

If you changed any of the network fields that will cause the node to reboot, the Change Network Configuration confirmation dialog box appears. If you changed a gateway setting, a confirmation appropriate to the gateway field appears. If you only changed the IP address fields, no confirmation dialog box appears.

Step 4 If a confirmation dialog box appears, click **Yes**.

If you changed an IP address, subnet mask length, or TCC CORBA (IIOP) Listener Port, both XTC cards will reboot, one at a time. Confirm that the changes appear. If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15327 Troubleshooting Guide*, as needed.

Step 5 Return to your originating procedure (NTP).

DLP-B142 Modify a Static Route

Purpose	Use this task to modify a static route on an ONS 15327.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Network** tabs.

Step 2 Click the **Static Routing** tab.

Step 3 Click the static route you want to edit.

Step 4 Click **Edit.**

Step 5 In the Edit Selected Static Route dialog box, enter the following:

- Mask
- Next Hop
- Cost

See the "DLP-B65 Create a Static Route" task on page 3-9 for detailed field descriptions.

Step 6 Click **OK**.

Step 7 Return to your originating procedure (NTP).

DLP-B143 Delete a Static Route

Purpose	Use this task to delete an existing static route on an ONS 15327.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Network** > **Static Routing** tabs.

Step 2 Click the static route you want to delete.

Step 3 Click **Delete**. A confirmation dialog box appears.

Step 4 Click **Yes**.

Step 5 Return to your originating procedure (NTP).

DLP-B144 Disable the Open Shortest Path First Protocol

Purpose	Use this task to disable the Open Shortest Path First (OSPF) routing protocol for an ONS 15327 LAN.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Network** > **OSPF** tabs. The OSPF subtab has several options.

Step 2 In the OSPF on LAN area, uncheck the **OSPF active on LAN** check box.

Step 3 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

Step 4 Return to your originating procedure (NTP).

Note Disabling OSPF can cause an XTC reboot, which causes a temporary loss of connectivity to the node, but does not affect traffic.

NTP-B202 Customize the CTC Network View

Purpose	Use this procedure to modify the CTC network view, including grouping nodes into domains for a less-cluttered display, changing the network view background color, and using a custom image for the network view background.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

Step 2 Complete the following tasks, as needed:

- DLP-B145 Change the Network View Background Color, page 10-8
- DLP-B267 Change the Default Network View Background Map, page 10-8
- DLP-B268 Apply a Custom Network View Background Map, page 10-9
- DLP-B148 Create Domain Icons, page 10-10
- DLP-B149 Manage Domain Icons, page 10-10

- DLP-B269 Enable Dialog Box Do-Not-Display Option, page 10-11

Stop. You have completed this procedure.

DLP-B145 Change the Network View Background Color

Purpose	This task changes the network view background color and the domain view background color (the area displayed when you open a domain).
Tools/Equipment	None
Prerequisite procedures	DLP-B60 Log into CTC, page 2-23
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note If you modify background colors, the change is stored in your CTC user profile on the local computer. The change does not affect other CTC users on different computers.

Step 1 From the View menu choose **Go to Network View**.

Step 2 Right-click the network view or domain map area and choose **Set Background Color** from the shortcut menu.

Step 3 On the Choose Color dialog box, select a background color.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-B267 Change the Default Network View Background Map

Purpose	This task changes the default map of the CTC network view.
Tools/Equipment	None
Prerequisite procedures	DLP-B60 Log into CTC, page 2-23
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note If you modify the background image, the change is stored in your CTC user profile on the local computer. The change does not affect other CTC users on different computers.

Step 1 From the View menu choose **Go to Network View**.

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

Step 3 On the Preferences dialog box, click the **Map** tab, then check the **Use Default Map** check box if it is not already checked.

Step 4 Click the **Default Maps** field and choose a default map from the pull-down menu. Map choices are: Germany, Japan, Netherlands, South Korea, United Kingdom, and the United States (default).

Step 5 Click **Apply**. The new network map is displayed.

Step 6 Click **OK**.

Step 7 If the ONS 15327 icons are not visible, right-click the network view and choose **Zoom Out**. Repeat until all the ONS 15327 icons are visible.

Step 8 If you need to reposition the node icons, drag and drop them one at a time to a new location on the map.

Step 9 If you want to change the magnification of the icons, right-click the network view and choose **Zoom In**. Repeat until the ONS 15327 icons are displayed at the magnification you want.

Step 10 Return to your originating procedure (NTP).

DLP-B268 Apply a Custom Network View Background Map

Purpose	This task changes the background image or map on the CTC network view.
Tools/Equipment	None
Prerequisite procedures	DLP-B60 Log into CTC, page 2-23
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note You can replace the network view background image with any JPEG or GIF image that is accessible on a local or network drive. If you apply a custom background image, the change is stored in your CTC user profile on the local computer. The change does not affect other CTC users on different computers.

Step 1 From the View menu choose **Go to Network View**.

Step 2 Right-click the network or domain map and choose **Set Background Image**.

Step 3 Click **Browse**. Navigate to the graphic file you want to use as a background.

Step 4 Select the file. Click **Open**.

Step 5 Click **Apply** and then click **OK**.

Step 6 If the ONS 15327 icons are not visible, right-click the network view and choose **Zoom Out**. Repeat this step until all the ONS 15327 icons are visible.

Step 7 If you need to reposition the node icons, drag and drop them one at a time to a new location on the map.

Step 8 If you want to change the magnification of the icons, right-click the network view and choose **Zoom In** or **Zoom Out**. Repeat this step until the ONS 15327 icons are displayed at the magnification you want.

Step 9 Return to your originating procedure (NTP).

DLP-B148 Create Domain Icons

Purpose	Use this task to create a domain icon to group ONS 15327 icons in CTC network view.
Tools/Equipment	None
Prerequisite procedures	DLP-B60 Log into CTC, page 2-23
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note All domain changes, such as added or removed nodes, are visible to all users who log into the network.

Step 1 From the View menu choose **Go to Network View**.

Step 2 Right-click the network map and choose **Create New Domain** from the shortcut menu.

Step 3 When the domain icon appears on the map, click the map name and type the domain name.

Step 4 Press **Enter**.

Step 5 Return to your originating procedure (NTP).

DLP-B149 Manage Domain Icons

Purpose	Use this task to manage CTC network view domain icons.
Tools/Equipment	None
Prerequisite procedures	DLP-B60 Log into CTC, page 2-23 DLP-B148 Create Domain Icons, page 10-10
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note All domain actions, such as adding or removing node icons, will be seen by all users who log into the network.

Step 1 From the View menu choose **Go to Network View**.

Step 2 Locate the domain action you want in Table 10-1 and complete the appropriate steps.

Table 10-1 Managing Domains

Domain action	Steps
Move a domain	Drag and drop the node icon to the new location.
Rename a domain	Right-click the domain icon and choose **Rename Domain** from the shortcut menu. Type the new name in the domain name field.
Add a node to a domain	Drag and drop the domain icon to the domain icon.
Move a node from a domain to the network map	Open the domain and right-click a node. Select **Move Node Back to Parent View**.
Open a domain	• Double-click the domain icon. • Right-click the domain and choose **Open Domain**.
Return to network view	Right-click the domain view area and choose **Go to Parent View** from the shortcut menu.
Preview domain contents	Right-click the domain icon and choose **Show Domain Overview**. The domain icon shows a small preview of the nodes in the domain. To turn off the domain overview, right-click the overview and select **Show Domain Overview**.
Remove domain	Right-click the domain icon and choose **Remove Domain**. Any nodes residing in the domain are returned to the network map.

Step 3 Return to your originating procedure (NTP).

DLP-B269 Enable Dialog Box Do-Not-Display Option

Purpose	Use this task to ensure that a user-selected "Do not display" dialog box preference is enabled for subsequent sessions or to disable the "Do not display" option.
Tools/Equipment	None
Prerequisite procedures	DLP-B60 Log into CTC, page 2-23
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note If any user who has rights to perform an operation (for example, creating a circuit) selects the "Do not show this dialog again" check box on a dialog box, the dialog box is not displayed for any other users who perform that operation on the network unless the command is overridden using the following task.

Step 1 From the Edit menu, choose **Preferences**.

Step 2 In the Preferences dialog box, click the **General** tab.

The Preferences Management area field lists all dialog boxes where "Do not show this dialog again" was checked.

Step 3 Choose one of the following:

- **Don't Show Any**—Hides all do-not-display check boxes.
- **Show All**—Overrides do-not-display check box selections and displays all dialog boxes.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

NTP-B203 Modify or Delete 1+1 Card Protection Settings

Purpose	Use this procedure to modify or delete 1+1 card protection settings.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Modifying and deleting protection groups can be service affecting.

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

Step 3 Perform any of the following tasks as needed:

- DLP-B154 Modify a 1+1 Protection Group, page 10-13
- DLP-B155 Delete a Protection Group, page 10-14

Step 4 Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

Stop. You have completed this procedure.

DLP-B154 Modify a 1+1 Protection Group

Purpose	Use this task to modify a 1+1 protection group for any optical port (OC-3, OC-12, or OC-48).
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Protection** tabs.

Step 2 Under Protection Groups, click the 1+1 protection group you want to modify.

Step 3 Under Selected Group, you can modify the following:

- Name—As needed, type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
- Bidirectional switching—As needed, check or uncheck
- Revertive—Check this check box if you want traffic to revert to the working card after failure conditions stay corrected for the amount of time chosen from the Reversion time menu. Uncheck if you do not want traffic to revert.
- Reversion time—If the Revertive check box is selected, choose the reversion time from the Reversion time pull-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card. Traffic can revert when conditions causing the switch are cleared.

See the "NTP-B170 Create Optical Protection Groups" procedure on page 3-20 for field descriptions.

Step 4 Click **Apply**. Confirm that the changes appear.

Note If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15327 Troubleshooting Guide*, as needed.

Step 5 Return to your originating procedure (NTP).

DLP-B155 Delete a Protection Group

Purpose	Use this task to delete a 1+1 protection group.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, click the **Provisioning** > **Protection** tabs.

Step 2 In the Protection Groups list, click the protection group you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Yes** in the Delete Protection Group dialog box to confirm deletion. Confirm that the changes appear; if they do not, repeat Steps 1 through 3.

Step 5 Return to your originating procedure (NTP).

NTP-B204 Delete a SONET DCC Termination

Purpose	Use this task to delete a SONET DCC termination on the ONS 15327.
Tools/Equipment	None
Prerequisite Procedures	DLP-B253 Provision SONET DCC Terminations, page 4-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Deleting a DCC termination can cause you to lose visibility of nodes that do not have other DCCs or network connections to the CTC computer.

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Provisioning > SONET DCC** tabs.

Step 3 Click the DCC termination you want to delete. Click **Delete**. The Delete SDCC Termination dialog box opens.

Step 4 Select the **Set Port Out of Service** check box, as needed, if you want to change the OC-N port where the DCC terminated to out of service (this may be service affecting).

Step 5 Click **Yes** to confirm. Confirm that the changes appear.

Stop. You have completed this procedure.

NTP-B85 Change Node Timing

Purpose	This procedure changes the SONET timing settings for the ONS 15327.
Tools/Equipment	None
Prerequisite Procedures	NTP-B28 Set Up Timing, page 3-16
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

Step 3 As needed, complete the "DLP-B157 Change the Node Timing Source" task on page 10-15.

Step 4 If you need to change any internal timing settings, follow the "DLP-B70 Set Up Internal Timing" task on page 3-19 for the settings you need to modify.

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

Step 5 If you need to verify timing after removing a node from a BLSR or a UPSR, see the "DLP-B195 Verify Timing in a Reduced Ring" task on page 13-12.

Step 6 Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

Stop. You have completed this procedure.

DLP-B157 Change the Node Timing Source

Purpose	This task changes the SONET timing source for the ONS 15327
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution The following procedure may be service affecting and should be performed during a scheduled maintenance window.

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 In the General Timing section, change any of the following information:

- Timing Mode

Note Because mixed timing can cause timing loops, Cisco does not recommend using the Mixed Timing option. Use this mode with care.

- SSM Message Set
- Quality of RES
- Revertive
- Reversion Time

See the "DLP-B69 Set Up External or Line Timing" task on page 3-17 for field descriptions.

Step 3 In the BITS Facilities section, you can change the following information:

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

- State
- Coding
- Framing
- Sync Messaging
- AIS Threshold
- LBO

Step 4 Under Reference Lists, you can change the following information:

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

- NE Reference
- BITS 1 Out/BITS 2 Out

Step 5 Click **Apply**. Confirm that the changes appear.

Note If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15327 Troubleshooting Guide*, as needed.

Step 6 Return to your originating procedure (NTP).

NTP-B205 Modify Users and Change Security

Purpose	Use this procedure to modify user and security properties for the ONS 15327.
Tools/Equipment	None
Prerequisite Procedures	NTP-B30 Create Users and Assign Security, page 3-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

Step 3 Perform any of the following tasks as needed:

- DLP-B271 Change Node Security Policy - Single Node, page 10-17
- DLP-B272 Change Node Security Policy - Multiple Nodes, page 10-18
- DLP-B158 Change User and Security Settings - Single Node, page 10-19
- DLP-B160 Change User and Security Settings - Multiple Nodes, page 10-20
- DLP-B159 Delete User - Single Node, page 10-22
- DLP-B161 Delete User - Multiple Nodes, page 10-22

Step 4 Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

Stop. You have completed this procedure.

DLP-B271 Change Node Security Policy - Single Node

Purpose	This task changes the security policy for a single node, including idle user timeouts, user lockouts, password changes, and concurrent login policies.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning** > **Security** > **Policy** tabs.

Step 2 Under Idle User Timeout, you can modify the timeout times by clicking the hour (H) and minute (M) arrows. You can choose values between 0 and 16 hours, and 0 and 59 minutes.

Step 3 Under User Lockout, you can modify the following:

- Failed Logins Before Lockout—The number of failed login attempts a user can make before the user is locked out from the node. You can choose a value between 0 and 10.

- Manual Unlock by Superuser—Allows a user with Superuser privileges to manually unlock a user who has been locked out from a node.
- Lockout Duration—Sets the amount of time the user will be locked out after a failed login. You can choose a value between 0 and 10 minutes, and 0 and 55 seconds (in five-second intervals).

Step 4 Under Concurrent Logins, click **Single Session Per User** if you want to limit users to a single login session.

Step 5 Under Password Change, you can modify the following:

- Require [nn] different passwords...—Choose a value between 0 and 10 to determine how many different passwords have to be created before a password can be reused.
- ...or a waiting period of [nn] days before password reuse—Choose a value between 0 and 30 days to set the amount of time (in days) before a password can be reused.

Users can change their passwords after they meet one of the two conditions. For example, if you set the number of different passwords to 5 and the number of days to 20, users can reuse a password after they change the password 5 times or after 20 days elapse, whichever occurs first.

Step 6 Click **Apply**. Confirm that the changes appear.

Step 7 Return to your originating procedure (NTP).

DLP-B272 Change Node Security Policy - Multiple Nodes

Purpose	This task changes the security policy for multiple nodes, including idle user timeouts, user lockouts, password change, and concurrent login policies.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 From the View menu choose **Go to Network View**.

Step 2 Click the **Provisioning** > **Security > Policy** tabs. A read-only table of nodes and their policies is displayed.

Step 3 Click a node on the table that you want to modify, then click the **Change** button.

Step 4 Under Idle User Timeout, you can modify the timeout times by clicking the hour (H) and minute (M) arrows. You can choose values between 0 and 16 hours, and 0 and 59 minutes.

Step 5 Under User Lockout, you can modify the following:

- Failed Logins Before Lockout—The number of failed login attempts a user can make before the user is locked out from the node. You can choose a value between 0 and 10.
- Manual Unlock by Superuser—Allows a user with Superuser privileges to manually unlock a user who has been locked out from a node.
- Lockout Duration—Sets the amount of time the user will be locked out after a failed login. You can choose a value between 0 and 10 minutes, and 0 and 55 seconds (in five-second intervals).

Step 6 Under Concurrent Logins, click **Single Session Per User** if you want to limit users to a single login session.

Step 7 Under Password Change, you can modify the following:

- Require [nn] different passwords...—Choose a value between 0 and 10 to determine how many different passwords have to be created before a password can be reused.
- ...or a waiting period of [nn] days before password reuse—Choose a value between 0 and 30 days to set the amount of time (in days) before a password can be reused.

Users can change their passwords after they meet one of the two conditions. For example, if you set the number of different passwords to 5 and the number of days to 20, users can reuse a password after they change their password 5 times or after 20 days elapse, whichever occurs first.

Step 8 Click **OK**.

Step 9 On the Security Policy Change Results dialog box, confirm the changes, then click **OK**.

Step 10 Return to your originating procedure (NTP).

DLP-B158 Change User and Security Settings - Single Node

Purpose	This task changes settings for an existing user at one node.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning** > **Security** > **Users** tabs.

Step 2 Click the user whose settings you want to modify.

Step 3 Click **Change**.

Step 4 In the Change User dialog box, enter the following:

- New Password
- Confirm New Password
- Security Level
- You can also lock out the user by selecting the check box.

See the“NTP-B30 Create Users and Assign Security” procedure on page 3-3 for field descriptions.

Step 5 Click **OK**.

Note User settings that you changed during this task will not appear until that user logs off and logs back in again.

Step 6 Return to your originating procedure (NTP).

DLP-B160 Change User and Security Settings - Multiple Nodes

Purpose	This task changes settings for an existing user on multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

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

Step 1 From the View menu, choose **Go to Network View**. Verify that all the nodes where you want to add users are accessible.

Step 2 Click the **Provisioning** > **Security > Users** tabs. Highlight the user's name whose settings you want to change.

Step 3 Click **Change**. The Change User dialog box appears.

Step 4 In the Change User dialog box, enter the following:

- New Password
- Confirm New Password
- Security Level
- You can also lock out the user by selecting the check box.

See the "DLP-B75 Create a New User - Multiple Nodes" task on page 3-4 for field descriptions.

Step 5 Click **OK**. A Change Results confirmation dialog box appears.

Step 6 Click **OK** to acknowledge the changes. Confirm that the changes appear; if not, repeat the task.

Step 7 Return to your originating procedure (NTP).

DLP-B315 Log Out a User - Single Node

Purpose	Use this task to log out a user from a single node.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 In node view, click the **Provisioning** > **Security** > **Active Logins** tabs.

Step 2 Choose the user you want to log out and click **Logout**.

Step 3 On the Logout User dialog box, check **Lockout before Logout** if you want to prevent the user from logging in after logout. Parameters set under User Lockouts in the Policy tab determine when the user can log back in. Either a manual unlock by a Superuser is required or the user is locked out for the amount of time specified in the Lockout Duration field. See the "DLP-B271 Change Node Security Policy - Single Node" task on page 10-17 for more information.

Step 4 Click **OK**.

Step 5 Click **Yes** to confirm the logout.

Step 6 Return to your originating procedure (NTP).

DLP-B316 Log Out a User - Multiple Nodes

Purpose	Use this task to log out a user from multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 From the view menu, chose **Go to Network View**.

Step 2 Click the **Provisioning** > **Security > Active Logins** tabs.

Step 3 Choose the user you want to log out.

Step 4 Click **Logout**.

Step 5 On the Logout User dialog box, check the nodes where you want to log out the user.

Step 6 Check **Lockout before Logout** if you want to prevent the user from logging in after logout. Parameters set under User Lockouts in the Policy tab determine when the user can log back in. Either a manual unlock by a Superuser is required or the user is locked out for the amount of time specified in the Lockout Duration field. See the "DLP-B271 Change Node Security Policy - Single Node" task on page 10-17 for more information.

Step 7 Click **OK**.

Step 8 Click **Yes** to confirm the logout.

Step 9 Return to your originating procedure (NTP).

DLP-B159 Delete User - Single Node

Purpose	Use this task to delete an existing user from a single node.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note CTC will allow you to delete other Superuser IDs if one Superuser ID remains. For example, you can delete the CISCO15 user if you have created another Superuser ID. Use this option with caution.

Note Users who are logged in when you delete them will not be logged out. The delete user action will take effect after the user logs out. To log out a user who is currently logged in, complete the "DLP-B315 Log Out a User - Single Node" task on page 10-20.

Step 1 In node view, select the **Provisioning** > **Security** > **Users** tabs.

Step 2 Choose the user you want to delete.

Step 3 Click **Delete**.

Step 4 In the Delete User dialog box, click **OK**. Confirm that the changes appear; if not, repeat the task.

Step 5 Return to your originating procedure (NTP).

DLP-B161 Delete User - Multiple Nodes

Purpose	Use this task to delete an existing user from multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note CTC will allow you to delete other Superuser IDs if one Superuser ID remains. For example, you can delete the CISCO15 user if you have created another Superuser ID. Use this option with caution.

Note Users who are logged in when you delete them will not be logged out. The delete user action will take effect after the user logs out. To log out a user who is currently logged in, complete the "DLP-B316 Log Out a User - Multiple Nodes" task on page 10-21.

Step 1 From the View menu choose **Go to Network View**.

Step 2 Click the **Provisioning** > **Security > Users** tabs. Highlight the name of the user you want to delete.

Step 3 In the Delete User dialog box, click **OK**. Confirm that the changes appear; if not, repeat the task.

Step 4 Click **OK**. A User Deletion confirmation dialog box appears.

Step 5 Click **OK** to acknowledge the changes. Confirm that the changes appear; if not, repeat the task.

Step 6 Return to your originating procedure (NTP).

NTP-B87 Change SNMP Settings

Purpose	Use this procedure to modify SNMP settings for the ONS 15327.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

Step 3 Perform any of the following tasks as needed:

- DLP-B273 Modify SNMP Trap Destination, page 10-24
- DLP-B163 Delete SNMP Trap Destinations, page 10-25
- DLP-B164 Delete Ethernet RMON Alarm Thresholds, page 10-25

Step 4 Complete the "NTP-B108 Back Up the Database" procedure on page 14-6.

Stop. You have completed this procedure.

DLP-B273 Modify SNMP Trap Destination

Purpose	Use this task to modify the SNMP trap destinations on an ONS 15327 including community name, default UDP port, SNMP trap version, and maximum traps per second.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **SNMP** tabs.

Step 2 Select a trap in the **Trap Destinations** dialog box.

For a description of SNMP traps, refer to the *Cisco ONS 15327 Reference Manual*.

Step 3 Type the SNMP community name in the Community Name field.

Note The community name is a form of authentication and access control. The community name assigned to the ONS 15327 is case-sensitive and must match the community name of the NMS.

Note The default UDP port for SNMP is 162.

Step 4 Set the Trap Version field for either SNMPv1 or SNMPv2.

Refer to your NMS documentation to determine which version to use.

Step 5 Set your maximum traps per second in the Max Traps per Second field.

Note The value is the maximum number of traps per second that will be sent to the SNMP manager. If the field is set to 0, all traps are sent.

Step 6 If you want to allow the ONS 15327 SNMP agent to accept SNMP SET requests on certain MIBs, select the **Allow SNMP Sets** check box. If the box is not checked, SET requests are rejected.

Step 7 Click **Apply**.

Step 8 SNMP settings are now configured. To view SNMP information for each node, highlight the node IP address in the Trap Destinations area of the Trap Destinations screen. Confirm that the changes appear.

Note If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15327 Troubleshooting Guide*, as needed.

Step 9 Return to your originating procedure (NTP).

DLP-B163 Delete SNMP Trap Destinations

Purpose	Use this task to delete SNMP trap destinations on an ONS 15327.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **SNMP** tabs.

Step 2 Under Trap Destinations, click the trap you want to delete.

Step 3 Click **Delete**. A confirmation dialog box appears.

Step 4 Click **Yes**. Confirm that the changes appear; if not, repeat the task.

Step 5 Return to your originating procedure (NTP).

DLP-B164 Delete Ethernet RMON Alarm Thresholds

Purpose	This task deletes remote monitoring (RMON) threshold crossing alarms for Ethernet ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning** > **Ether Bridge** > **Thresholds** tabs.

Step 2 Click the RMON alarm threshold you want to delete.

Step 3 Click **Delete**. The Delete Threshold dialog box opens.

Step 4 Click **Yes** to delete that threshold.

Step 5 Return to your originating procedure (NTP).

CHAPTER 11

Upgrade Cards and Spans

This chapter explains how to upgrade the XTC card and how to upgrade optical speeds within a ring or protection group.

Before You Begin

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-B229 Upgrade the XTC-14 Card to XTC-28 Card, page 11-1—Complete this procedure as needed to upgrade the XTC-14 card to the XTC-28 card.
2. NTP-B94 Upgrade Optical Spans Automatically, page 11-3—Complete this procedure as needed to upgrade optical cards within UPSRs, BLSRs, and 1+1 protection groups.
3. NTP-B95 Upgrade Optical Spans Manually, page 11-5—Complete this procedure as needed to perform error recovery for the Span Upgrade Wizard or back out of a span upgrade (downgrade).

NTP-B229 Upgrade the XTC-14 Card to XTC-28 Card

Purpose	This procedure upgrades the XTC-14 card to the XTC-28 card. The procedure is non-service affecting; the upgrade will cause a protection switch of less than 50 ms in duration.
Tools/Equipment	Two XTC-28 cards
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note The UNEQ-P alarm might be raised during the upgrade if you have E10/E100-4 cards in the node. The alarm will appear and clear within a few seconds.

Note The MEA (card mismatch) alarm appears because CTC recognizes a mismatch between XTC card types. Disregard this alarm; it clears by the end of the procedure.

Step 1 Complete the "NTP-B108 Back Up the Database" procedure on page 14-6 before beginning the upgrade.

Step 2 Determine which XTC-14 card is the standby card. An amber ACT/STBY LED on the card faceplate indicates a standby card.

Step 3 Physically replace the standby XTC-14 card on the ONS 15327 with an XTC-28 card:

a. Open the XTC-14 card ejector.

b. Slide the card out of the slot. This raises an IMPROPRMVL alarm which will clear when the upgrade is complete. Ensure that traffic is flowing over the 14 DS-1 ports. Abnormal alarms will indicate if there is a problem with traffic. Ensure that the alarm filter is not selected when you are checking for abnormal alarms.

c. Open the ejector on the XTC-28 card.

d. Slide the XTC-28 card into the slot along the guide rails.

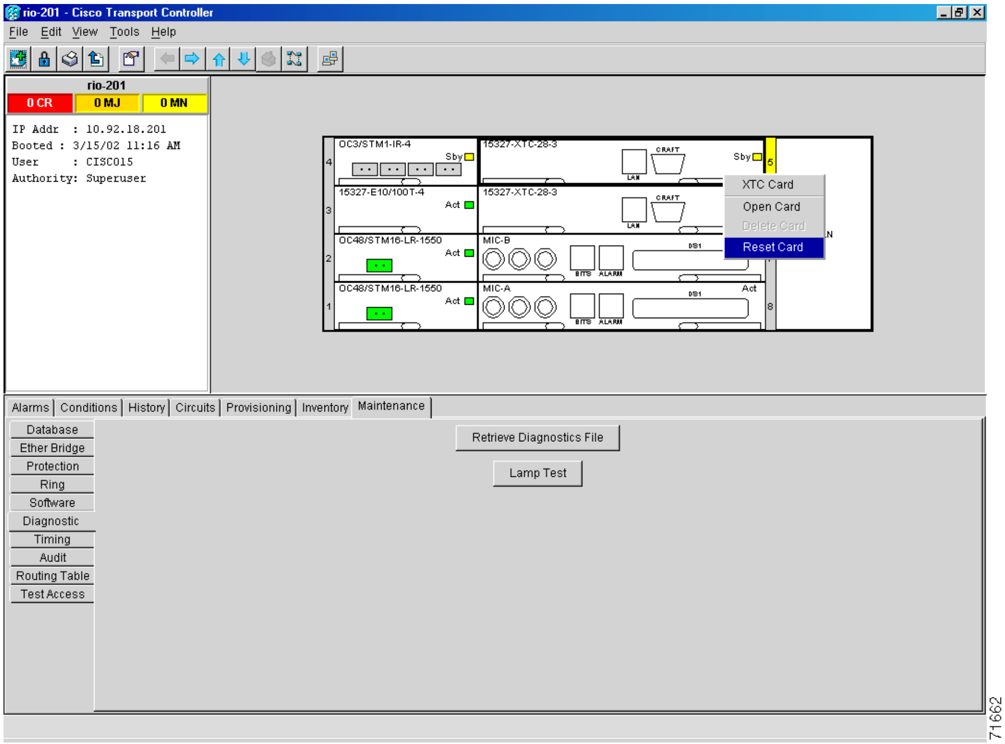
e. Close the ejector and secure the screw.

f. The ONS 15327 boots up the XTC-28 card. The XTC-28 card must copy the database, which can take approximately 10 minutes. Do not remove the card from the shelf during a database transfer.

Note The LEDs will flash while the XTC-28 is loading.

Step 4 After the XTC-28 has finished synchronizing its software and database and is in standby mode, in node view right-click the active XTC-14 and choose **Reset** from the drop-down menu (Figure 11-1).

Figure 11-1 Resetting the XTC card



IP Addr : 10.92.18.201
Booted : 3/15/02 11:16 AM
User : CISCO15
Authority: Superuser

Step 5 Physically replace the remaining XTC-14 card:

a. Open the XTC-14 card ejector.

b. Slide the card out of the slot. This raises an IMPROPRMVL alarm that will clear when the upgrade is complete.

c. Open the ejector on the XTC-28 card.

d. Slide the XTC-28 card into the slot along the guide rails.

e. Close the ejector and secure the screw.

f. The ONS 15327 boots up the second XTC-28 card. The second XTC-28 card must also copy the database, which can take approximately 10 minutes. Do not remove the card from the shelf during a database transfer.

Step 6 If power-related alarms occur after the second XTC-28 card is installed, check the voltage on the backplane. See the "DLP-B33 Measure Voltage" task on page 1-49 for instructions. Refer to the *Cisco ONS 15327 Troubleshooting Guide* for information on clearing alarms.

Stop. You have completed this procedure.

NTP-B94 Upgrade Optical Spans Automatically

Purpose	This procedure upgrades OC-N speeds within BLSRs, UPSRs, and 1+1 protection groups using the Span Upgrade Wizard. Upgrading a span is non-service affecting and will cause no more than three switches, each of which is less than 50 ms in duration.
Tools/Equipment	Replacement cards
Prerequisite Procedures	The span upgrade procedure requires at least two technicians (one at each end of the span) who can communicate with each other during the upgrade.
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

Caution Do not perform any other maintenance operations or add any circuits during a span upgrade.

Note The Span Upgrade option will only be visible and available if the hardware necessary for the upgrade is present.

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

Step 2 Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, SD, and FORCED-REQ-RING are present. See the "DLP-B298 Check the Network for Alarms and Conditions" task on page 12-3 for instructions.

Step 3 In network view, right-click the span you want to upgrade.

Step 4 Choose **Span Upgrade** from the drop-down menu.

Step 5 The first Span Upgrade dialog box appears. Follow the instructions on the dialog box and the wizard will lead you through the rest of the span upgrade.

Caution As indicated by the wizard, when installing cards you must wait for the cards to boot up and become active before proceeding to the next step.

Note The Back button is only enabled in the first screen of the wizard; because you cannot back out of an upgrade via the wizard, close the wizard and initiate the manual procedure if you need to back out of the upgrade at any point beyond the second screen.

Note Remember to attach the fiber after installing the OC-N cards.

Step 6 Repeat Steps 2 through 5 for additional spans in the ring.

Note Optical transmit and receive levels should be in their acceptable range as shown in the specifications section for each card in the *Cisco ONS 15327 Reference Manual*.

Note The span upgrade process resets the line CV-L threshold to the factory default. The CV-L threshold is reset because the threshold is dependent on line rate.

Note Span upgrades do not upgrade SONET topologies; for example, 1+1 protection group to a two-fiber BLSR.

Note During the upgrade/downgrade some minor alarms and conditions display and then clear automatically. No service-affecting alarms (SA, Major, or Critical) should occur other than BLSR Out of Sync, which will clear when the upgrade/downgrade of all nodes is complete. If any other service-affecting alarms occur, Cisco recommends backing out of the procedure. Extra time may be required to clear all of the Out of Sync alarms depending on the size of the BLSR.

Stop. You have completed this procedure.

NTP-B95 Upgrade Optical Spans Manually

Purpose	This procedure upgrades OC-N speeds within BLSRs, UPSRs, and 1+1 protection groups by upgrading OC-N cards. Upgrading a span is non-service affecting and will cause no more than three switches, each of which is less than 50 ms in duration.
Tools/Equipment	Replacement cards
Prerequisite Procedures	The manual span upgrade procedure requires at least two technicians (one at each end of the span) who can communicate with each other during the upgrade.
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note Optical card transmit and receive levels should be in their acceptable range as shown in the specifications section for each card in the *Cisco ONS 15327 Reference Manual*.

Note In this context the word "span" represents the optical path between two nodes. The words "span endpoint" represent the nodes on each end of a span.

Note If any of the XTC cards reboot during the span upgrade, you must manually reset each one when the span upgrade procedure is complete for all the nodes in the ring. See the "NTP-B113 Reset the XTC Using CTC" procedure on page 14-23 for card reset procedures.

Step 1 Determine the type of span you need to upgrade and make sure you have the necessary cards. Valid span upgrades include:

- OC-12 to OC-48
- OC-12 IR to OC-12 LR
- OC-48 IR to OC-48 LR

Step 2 Complete the "DLP-B60 Log into CTC" task on page 2-23. The node (default) view appears. If you are already logged in, continue with Step 3.

Step 3 Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, SD, and FORCED-REQ-RING are present. See the "DLP-B298 Check the Network for Alarms and Conditions" task on page 12-3 for instructions.

Note During the upgrade/downgrade some minor alarms and conditions display and then clear automatically. No service-affecting alarms (SA, Major, or Critical) should occur other than BLSR Out-of-Sync, which will clear when the upgrade/downgrade of all nodes is complete. If any other service-affecting alarms occur, Cisco recommends backing out of the procedure. Allow extra time for a large BLSR to clear all of the Out-of-Sync alarms.

Step 4 Complete a manual upgrade task if you need to perform error recovery for the Span Upgrade Wizard or back out of a span upgrade (downgrade):

- Complete the "DLP-B293 Perform a Manual Span Upgrade on a Two-Fiber BLSR" task on page 11-6 to upgrade an optical span manually within a two-fiber BLSR.
- Complete the "DLP-B295 Perform a Manual Span Upgrade on a UPSR" task on page 11-8 to upgrade an optical span manually within a UPSR.
- Complete the "DLP-B296 Perform a Manual Span Upgrade on a 1+1 Protection Group" task on page 11-9 to upgrade an optical span manually within a 1+1 protection group.
- Complete the "DLP-B297 Perform a Manual Span Upgrade on an Unprotected Span" task on page 11-11 to upgrade an unprotected optical span manually.

Note The span upgrade process resets the line's CV-L threshold to factory default. The CV-L threshold is reset because the threshold is dependent on line rate.

Note Span upgrades do not upgrade SONET topologies; for example, 1+1 protection group to a two-fiber BLSR.

Note The Span Upgrade option will only be visible and available if the hardware necessary for the upgrade is present.

Stop. You have completed this procedure.

DLP-B293 Perform a Manual Span Upgrade on a Two-Fiber BLSR

Purpose	This task upgrades a two-fiber BLSR span to a higher optical rate.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

Caution Do not perform any other maintenance operations or add any circuits during a span upgrade.

Note If any of the XTC cards reboot during the span upgrade, you must manually reset each one when the span upgrade procedure is complete for all the nodes in the ring. See the "NTP-B113 Reset the XTC Using CTC" procedure on page 14-23 for card reset procedures.

Note All spans connecting the nodes in a BLSR must be upgraded before the bandwidth is available.

Step 1 Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, SD, and FORCED-REQ-RING are present on the BLSR that you will upgrade. See the "DLP-B298 Check the Network for Alarms and Conditions" task on page 12-3 for instructions.

Step 2 Apply a Force switch to both span endpoints (nodes) on the span that you will upgrade first. See "DLP-B303 Initiate a BLSR Force Ring Switch" task on page 13-6.

Step 3 Remove the fiber from both endpoints and ensure that traffic is still running.

Step 4 Remove the OC-N cards from both endpoints.

Step 5 At one endpoint, in node view right-click the OC-N card and choose **Change Card**.

Step 6 In the Change Card dialog box, choose the new OC-N card type.

Step 7 Click **OK**.

Step 8 Repeat Steps 5 through 7 at the second endpoint.

Step 9 Install the new OC-N cards in both endpoints before attaching the fiber to the newly installed OC-N cards. Check that the receive signal falls within the acceptable range. Wait for the IMPROPRMVL alarm to clear and the cards to become active.

Step 10 When cards in both endpoint nodes have been successfully upgraded and all facility alarms (LOS, SD or SF) are cleared, complete the "DLP-B194 Clear a BLSR Force Ring Switch" task on page 13-8 at both endpoints.

The Force switch clears and traffic is running. If you have lost traffic, make sure the cabling is installed properly. See the "NTP-B221 Install Optical Cables" procedure on page 1-40. If this does not resolve the problem, perform a downgrade. The procedure for downgrading is the same as upgrading except that you choose a lower-rate card in Step 6 and install a lower-rate card in Step 9.

Step 11 Repeat this task for each span in the BLSR. When you are done with each span, the upgrade is complete.

Step 12 Return to your originating procedure (NTP).

DLP-B295 Perform a Manual Span Upgrade on a UPSR

Purpose	This task upgrades UPSR spans to a higher optical speed. Repeat the task to upgrade each span, and thus the entire ring, to the higher optical rate.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

Caution Do not perform any other maintenance operations or add any circuits during a span upgrade.

Note If any of the XTC cards reboot during the span upgrade, you must manually reset each one, once the span upgrade procedure is complete for all the nodes in the ring. See the "NTP-B113 Reset the XTC Using CTC" procedure on page 14-23 for card reset procedures.

Step 1 Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, SD, and FORCED-REQ-RING are present on the span that you will upgrade. See the "DLP-B298 Check the Network for Alarms and Conditions" task on page 12-3 for instructions.

Step 2 Complete the "DLP-B197 Initiate a UPSR Force Switch" task on page 13-16 on the span that you will upgrade at both endpoints.

Step 3 Remove the fiber from both endpoint nodes in the span and ensure that traffic is still running.

Step 4 Remove the OC-N cards from both span endpoints.

Step 5 At one endpoint, in node view right-click the OC-N card and choose **Change Card**.

Step 6 In the Change Card dialog box, choose the new OC-N card type.

Step 7 Click **OK**.

Step 8 Before attaching the fiber to the newly installed OC-N cards, check that the receive signal falls within the acceptable range. Install the new OC-N cards in both endpoints and attach the fiber to the cards. Wait for the IMPROPRMVL alarm to clear and the cards to become active.

Step 9 Complete the "DLP-B198 Clear a UPSR Switch" task on page 13-17 at both endpoints when cards in both nodes have been successfully upgraded and all the facility alarms (LOS, SD or SF) are cleared.

The Force switch clears and traffic is running. If you have lost traffic, make sure the cabling is installed properly. See the "NTP-B221 Install Optical Cables" procedure on page 1-40. If this does not resolve the problem, perform a downgrade. The procedure for downgrading is the same as upgrading except that you choose a lower-rate card in Step 6 and install a lower-rate card in Step 8.

Step 10 Return to your originating procedure (NTP).

DLP-B296 Perform a Manual Span Upgrade on a 1+1 Protection Group

Purpose	This task upgrades a linear 1 + 1 span to a higher optical rate.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

Caution Do not perform any other maintenance operations or add any circuits during a span upgrade.

Note If any of the XTC cards reboot during the span upgrade, you must manually reset each one when the span upgrade procedure is complete for all the nodes in the ring. See the "NTP-B113 Reset the XTC Using CTC" procedure on page 14-23 for card reset procedures.

Step 1 Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, SD, and FORCED-REQ-RING are present on the span that you will upgrade. See the "DLP-B298 Check the Network for Alarms and Conditions" task on page 12-3 for instructions.

Step 2 Apply a Force switch on the ports that you will upgrade, beginning with the protect port:

a. In node view, click the **Maintenance > Protection** tabs.

b. Under Protection Groups, choose the 1+1 protection group.

c. Under Selected Group, choose the protect port (regardless if it is active or standby).

d. From Switch Commands, click **Force**.

e. Click **Yes** on the confirmation dialog box.

Note If the switching mode is bidirectional in the 1+1 protection group, apply the Force command to only one end of the span. If the Force command is applied to both ends when the switching mode is bidirectional, a switch of more than 50 ms in duration will result.

Note A Force switch request on a span or card (port) causes CTC to raise a FORCED-REQ condition. It is informational only; the condition will clear when the force switch command is cleared.

Step 3 Repeat Step 2 for each port you will upgrade.

Step 4 Remove the fiber from both ends of the span and ensure that traffic is still running.

Step 5 Remove the OC-N cards from both span endpoints.

Step 6 At one endpoint, in node view, right-click the OC-N slot and choose **Change Card**.

Step 7 In the Change Card dialog box, choose the new OC-N card type.

Step 8 Click **OK**.

Step 9 Repeat Steps 5 through 7 at the second endpoint.

Step 10 Install the new OC-N cards in both endpoints before attaching the fiber to the newly installed OC-N cards, check that the receive signal falls within the acceptable range. Wait for the IMPROPRMVL alarm to clear and the cards to become standby.

Step 11 When cards on each end of the span have been successfully upgraded and all the facility alarms (LOS, SD or SF) are cleared, remove the Force switch:

a. In node view, click the **Maintenance > Protection** tabs.

b. Under Protection Groups, choose the 1+1 protection group.

c. Under Selected Group, choose the port with the force on it.

d. From Switch Commands, click **Clear**.

e. Click **Yes** on the confirmation dialog box.

The Force switch clears and traffic is running. If you have lost traffic, make sure the cabling is installed properly. See the "NTP-B221 Install Optical Cables" procedure on page 1-40. If this does not resolve the problem, perform a downgrade. The procedure for downgrading is the same as upgrading except that you choose a lower-rate card in Step 7 and install a lower-rate card in Step 9.

Step 12 Repeat this task for any other spans in the 1 + 1 linear configuration.

Step 13 Return to your originating procedure (NTP).

DLP-B297 Perform a Manual Span Upgrade on an Unprotected Span

Purpose	This task manually upgrades unprotected spans to a higher optical rate.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

Caution Upgrading unprotected spans will cause all traffic running on those spans to be lost.

Caution Do not perform any other maintenance operations or add any circuits during a span upgrade.

Note If any of the XTC cards reboot during the span upgrade, you must manually reset each one when the span upgrade procedure is complete for all the nodes in the ring. See the "NTP-B113 Reset the XTC Using CTC" procedure on page 14-23 for card reset procedures.

Step 1 Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, and SD, are present on the span that you will upgrade. See the "DLP-B298 Check the Network for Alarms and Conditions" task on page 12-3 for instructions.

Step 2 Remove the fiber from both endpoint nodes in the span.

Caution Removing the fiber will cause all traffic on the unprotected span to be lost.

Step 3 Remove the OC-N cards from both span endpoints.

Step 4 At one endpoint, in node view, right-click each OC-N slot and choose **Change Card**.

Step 5 In the Change Card dialog box, choose the new OC-N type.

Step 6 Click **OK**.

Step 7 Repeat Steps 4 through 6 at the second endpoint.

Step 8 Install the new OC-N cards in both endpoints and attach the fiber to the cards. Wait for the IMPROPRMVL alarm to clear and the cards to become active.

Step 9 Return to your originating procedure (NTP).

CHAPTER 12

Convert Network Configurations

This chapter explains how to convert from one SONET topology to another. For initial network turn up, see Chapter 4, "Turn Up Network."

Before You Begin

Before performing any of the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15327 Troubleshooting Guide* as necessary.

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-B154 Convert a Point-to-Point to a Linear ADM, page 12-1—Complete as needed.
2. NTP-B155 Convert a Point-to-Point or a Linear ADM to a Two-Fiber BLSR, page 12-3—Complete as needed.
3. NTP-B156 Convert a Point-to-Point or Linear ADM to a UPSR, page 12-6—Complete as needed.
4. NTP-B210 Convert a USPR to a Two-Fiber BLSR, page 12-6—Complete as needed.
5. NTP-B159 Modify a BLSR, page 12-8—Complete as needed.

NTP-B154 Convert a Point-to-Point to a Linear ADM

Purpose	This procedure upgrades a point-to-point configuration (two nodes) to a linear add/drop multiplexer (ADM) configuration (3 or more nodes).
Tools/Equipment	None
Prerequisite Procedures	The node that will be added must have OC-N cards installed. See Chapter 1, "Install Hardware," and Chapter 3, "Turn Up Node," for procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note Optical transmit and receive levels should be in their acceptable range as shown in the specifications section for each card in Table 8-3 on page 8-16.

Note In a point-to-point configuration, two OC-N cards are connected to two OC-N cards on a second node.

Step 1 Log into a point-to-point node. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. If you are already logged in, go to Step 2.

Step 2 Check the point-to-point network for alarms and conditions. Ensure that the alarm filter is not turned on. See the "DLP-B298 Check the Network for Alarms and Conditions" task on page 12-3 for instructions.

Step 3 Log into the node that will be added to the point-to-point configuration.

Step 4 Complete the "NTP-B24 Verify Card Installation" procedure on page 3-2 to ensure that the new node has two OC-N cards with the same rate as the point-to-point nodes.

Step 5 Complete the "NTP-B35 Verify Node Turn Up" procedure on page 4-2 for the new node.

Step 6 Physically connect the fibers between the point-to-point node and the new node.

Step 7 On the new node, create a 1+1 protection group for the OC-N cards that will connect to the point-to-point node. See the "NTP-B170 Create Optical Protection Groups" procedure on page 3-20 for instructions.

Step 8 Complete the "DLP-B253 Provision SONET DCC Terminations" task on page 4-4 for the working OC-N cards in the new node that will connect to the linear ADM network. Make sure to set the Port State in the Create SDCC Termination dialog box to IS.

Note Data Communications Channel (DCC) failure alarms appear until you create DCC terminations in the point-to-point node.

Step 9 Display the point-to-point node that will connect to the new node in CTC node view.

Step 10 Ensure that the point-to-point node has OC-N cards installed that can connect to the new node.

Step 11 Create a 1+1 protection group for the OC-N cards that will connect to the new node. See the "NTP-B170 Create Optical Protection Groups" procedure on page 3-20 for instructions.

Step 12 Create DCC terminations on the working OC-N card that will connect to the new node. See the "DLP-B253 Provision SONET DCC Terminations" task on page 4-4. In the Create SDCC Termination dialog box, set the port state to **IS**.

Step 13 Display the new node in node view.

Step 14 Complete the "NTP-B28 Set Up Timing" procedure on page 3-16 for the new node. If the new node is using line timing, set the working OC-N card as the timing source.

Step 15 Display the network view to verify that the newly created linear ADM configuration is correct. Two green span lines should appear between each linear node.

Step 16 Click the **Alarms** tab. Verify that no unexpected alarms are displayed. Ensure that the alarm filter is not turned on.

Step 17 Repeat the procedure to add an additional node to the linear ADM.

Stop. You have completed this procedure.

DLP-B298 Check the Network for Alarms and Conditions

Purpose	This task verifies that no alarms or conditions exist on the network.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	Retrieve or higher

Step 1 From the View menu, choose **Go to Network View**. Verify that all affected spans on the network map are green.

Step 2 A second verification method can be performed from the Conditions tab. Click **Retrieve Conditions** and verify that no switches are active. Make sure the Filter button is not selected.

Step 3 Click the **Alarms** tab. Verify that no critical or major alarms are present, nor any facility alarms, such as LOS, LOF, AIS-L, AIS-P, SF, and SD. Make sure the Filter button is not selected.

If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See Chapter 6, "Manage Alarms," or, if necessary, refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 4 Return to your originating procedure (NTP).

NTP-B155 Convert a Point-to-Point or a Linear ADM to a Two-Fiber BLSR

Purpose	This procedure upgrades a point-to-point configuration or linear ADM to a two-fiber Bidirectional Line Switched Ring (BLSR).
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution This procedure is service affecting.

Note Optical transmit and receive levels should be in their acceptable range as shown in the specifications section for each card in the *Cisco ONS 15327 Reference Manual*.

Step 1 Log into one of the nodes that you want to convert from a point-to-point or ADM to a BLSR. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. If you are already logged in, go to Step 2.

Step 2 Check for alarms and conditions. See the "DLP-B298 Check the Network for Alarms and Conditions" task on page 12-3 for instructions.

Step 3 Right-click a span adjacent to the node you are logged into.

Step 4 From the popup window, click **Circuits**. The Circuits on Span window appears.

Step 5 Verify that the total number of active STS circuits does not exceed 50 percent of the span bandwidth. In the Circuits column there is a block titled "Unused." This number should exceed 50 percent of the span bandwidth.

Note If the span is an OC-48, no more than 24 STSs can be provisioned on the span. If the span is an OC-12, no more than 6 STSs can be provisioned on the span.

Warning **If the first half of the capacity is exceeded, this procedure cannot be completed. Bandwidth must be 50 percent unassigned to convert to BLSR. Refer to local procedures for relocating circuits if these requirements are not met.**

Step 6 Repeat Steps 3 through 5 for each node in the point-to-point or linear ADM that you will convert to BLSR. If all nodes comply with Step 5, proceed to Step 7.

Step 7 Complete the "DLP-B189 Verify that a 1+1 Working Slot is Active" task on page 12-5 for every 1+1 protection group that supports a span in the point-to-point or linear ADM network.

Step 8 Complete the "DLP-B155 Delete a Protection Group" task on page 10-14 at each node that supports the point-to-point or linear ADM span.

Step 9 Complete the "DLP-B214 Change the Service State for a Port" task on page 4-5 to put the protect ports out of service at each node that supports the linear ADM span.

Step 10 (Linear ADM only) Physically remove the protect fibers from all nodes in the linear ADM.

Step 11 Create the ring by connecting the protect fiber from one end node to the protect port on the other end node.

Note If you need to physically remove any OC-N cards, do so now. See the "NTP-B219 Remove and Replace a Card" procedure on page 1-26.

Step 12 From the network view, click the **Circuits** tabs and complete the "DLP-B139 Export CTC Data" task on page 6-3 to save the circuit data to a file on your hard drive.

Step 13 Complete the "DLP-B253 Provision SONET DCC Terminations" task on page 4-4 at the end nodes; provision the slot in each node that is not already in the SDCC Terminations list.

Caution Deleting circuits is service affecting.

Step 14 For circuits provisioned on an STS that is now part of the protection bandwidth (STSs 7 to 12 for an OC-12 BLSR, and STSs 25 to 48 for an OC-48 BLSR), delete and recreate each circuit:

a. Complete the "NTP-B152 Delete Circuits" procedure on page 8-13 for one circuit.

b. Create the circuit on STSs 1 to 6 for an OC-12 BLSR, or on STSs 1 to 24 for an OC-48 BLSR on the fiber that served as the protect fiber in the linear ADM. See the "NTP-B189 Create a Manually Routed Optical Circuit" procedure on page 5-38 for instructions.

c. Repeat Steps a and b for each circuit residing on a BLSR protect STS.

Step 15 Complete the "NTP-B126 Create a BLSR" procedure on page 4-14 to put the nodes into a BLSR.

Stop. You have completed this procedure.

DLP-B189 Verify that a 1+1 Working Slot is Active

Purpose	This task verifies that a working slot in a 1+1 protection scheme is active (and that the protect slot is in standby).
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Both
Security Level	Maintenance or higher

Step 1 In the node view, click the **Maintenance > Protection** tabs.

Step 2 In the Selected Group pane, verify that the working slot/port is shown as Working/Active. If so, this task is complete.

Step 3 If the working slot says Working/Standby, manually switch traffic to the working slot:

a. In the Selected Group pane, choose the Protect/Active slot.

b. In the Switch Commands field, choose **Manual**.

c. Click **Yes** in the confirmation dialog box.

Step 4 Verify that the working slot is carrying traffic (Working/Active).

Note If the slot is not active, look for conditions or alarms that might be preventing the card from carrying working traffic. Refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 5 When the working slot is carrying traffic, clear the manual switch:

a. In the Switch Commands field, choose **Clear**.

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

Step 6 Verify that the working slot does not switch back to Standby, which might indicate a problem on the working span.

Step 7 Return to your originating procedure (NTP).

NTP-B156 Convert a Point-to-Point or Linear ADM to a UPSR

Purpose	This procedure upgrades a point-to-point system to a Unidirectional Path Switched Ring (UPSR).
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution This procedure is service affecting. All circuits are deleted and reprovisioned.

Step 1 Log into a node on the point-to-point or linear ADM. See the "DLP-B60 Log into CTC" task on page 2-23.

Step 2 Check for alarms and conditions. See the "DLP-B298 Check the Network for Alarms and Conditions" task on page 12-3 for instructions.

Step 3 Complete the "DLP-B189 Verify that a 1+1 Working Slot is Active" task on page 12-5 for each node.

Step 4 Complete the "DLP-B155 Delete a Protection Group" task on page 10-14 for each 1+1 protection group that supports the point-to-point or linear ADM span.

Step 5 Complete the "DLP-B253 Provision SONET DCC Terminations" task on page 4-4 at the protect cards in all nodes.

Step 6 Complete the "NTP-B152 Delete Circuits" procedure on page 8-13 and the "NTP-B188 Create an Automatically Routed Optical Circuit" procedure on page 5-35 to delete and recreate the circuits one at a time.

Caution Deleting circuits is service affecting.

Stop. You have completed this procedure.

NTP-B210 Convert a USPR to a Two-Fiber BLSR

Purpose	This procedure converts a UPSR to a two-fiber BLSR.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Both
Security Level	Provisioning or higher

Caution This procedure is service affecting. All circuits on the ring are deleted and reprovisioned.

Caution Read through this procedure completely before beginning the conversion.

Note Prior to beginning this procedure, you should have a unique ring ID number to identify the new BLSR and a unique node ID number for each node on the ring.

Note Prior to beginning this procedure, optical transmit and receive levels should be in their acceptable range as shown in the specifications section for each card in the *Cisco ONS 15327 Reference Manual*.

Step 1 Log into an ONS 15327 on the network where you will begin the ring conversion. See the "DLP-B60 Log into CTC" task on page 2-23.

Step 2 Check for alarms and conditions. See the "DLP-B298 Check the Network for Alarms and Conditions" task on page 12-3 for instructions.

Step 3 Click **View > Go to Network View**.

Step 4 Right-click a span adjacent to the node you are logged into.

Step 5 From the popup window, click **Circuits**. The Circuits on Span window appears.

Step 6 Verify that the total number of active STS circuits does not exceed 50 percent of the span bandwidth. In the Circuits column there is a block titled "Unused." This number should exceed 50 percent of the span bandwidth.

Note If the span is an OC-48, no more than 24 STSs can be provisioned on the span. If the span is an OC-12, no more than 6 STSs can be provisioned on the span.

Warning **If the first half of the capacity is exceeded, this procedure cannot be completed. Bandwidth must be 50 percent unassigned to convert to BLSR. Refer to local procedures for relocating circuits if these requirements are not met.**

Step 7 Repeat Steps 1 through 6 for each node in the UPSR that you will convert to BLSR. If all nodes comply with
Step 6, proceed to Step 8.

Step 8 Save all circuit information:

a. In network view, click the **Provisioning > Circuits** tabs.

b. Record the circuit information using one of the following tasks:

- From the File menu, click **Print** to print the circuits table.
- From the File menu, click **Export** and choose the data format: HTML, CSV (comma separated values), or TSV (tab separated values). Click **OK** and save the file in a temporary directory.

  See the "NTP-B195 Document Existing Provisioning" procedure on page 6-2 for more information.

Note This method uses the network view. To delete circuits one at a time from each node, see the "NTP-B152 Delete Circuits" procedure on page 8-13.

Step 9 Delete the circuits:

a. From network view, click the **Circuits** tab. All circuits on the ring appear.

b. With the **Shift** key pressed, click each circuit in the display. Each line in the display turns dark blue as it is selected.

c. After all circuits have been selected, click **Delete**. Allow several minutes for processing; the actual length of time depends on the number of circuits in the network.

Step 10 Complete the "NTP-B126 Create a BLSR" procedure on page 4-14 to create the BLSR.

Step 11 Complete the "NTP-B175 BLSR Acceptance Test" procedure on page 4-16.

Step 12 To recreate the circuits, see Chapter 5, "Create Circuits and VT Tunnels" and choose the applicable procedure for the circuit type you want to enter.

Stop. You have completed this procedure.

NTP-B159 Modify a BLSR

Purpose	This procedure changes a BLSR ID, node ID, or ring and span reversion times.
Tools/Equipment	None
Prerequisite Procedures	NTP-B126 Create a BLSR, page 4-14
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Log into a node in the BLSR you want to modify. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions.

Step 2 Check the BLSR for outstanding alarms and conditions. See the "DLP-B298 Check the Network for Alarms and Conditions" task on page 12-3 for instructions.

Note Some or all of the following alarms display during BLSR setup: E-W MISMATCH, RING MISMATCH, APSCIMP, APSDFLTK, and BLSROSYNC. The alarms clear after you configure all the nodes in the BLSR. For definitions of these alarms, see the *Cisco ONS 15327 Troubleshooting Guide*.

Step 3 To change the BLSR ring ID or the ring or span reversion times, complete the following steps. If you want to change a node ID, go to Step 4.

a. Switch to network view and click the **Provisioning > BLSR** tabs.

b. Click the BLSR you want to modify and click **Edit**.

c. In the BLSR window, change any of the following:
  - Ring ID—If needed, change the BLSR ring ID (a number between 0 and 9999). Do not choose a number that is already assigned to another BLSR.
  - Reversion time—If needed, change the amount of time that will pass before the traffic reverts to the original working path after a ring switch.

d. Click **Apply**.

e. If you changed the ring ID, the BLSR window closes automatically. If you only changed a reversion time, close the window by choosing **Close** from the File menu.

Step 4 To change a BLSR node ID, complete the following steps; otherwise, proceed to Step 5.

a. On the network map, double-click the node with the node ID you want to change.

b. Click the **Provisioning > BLSR** tabs.

c. Choose a Node ID number. Do not choose a number already assigned to another node in the same BLSR.

d. Click **Apply**.

Step 5 Switch to network view and verify the following:

- A green span line appears between all BLSR nodes.
- All E-W MISMATCH, RING MISMATCH, APSCIMP, DFLTK, BLSROSYNC, and Node ID Mismatch alarms are cleared. Ensure that the alarm filter is not turned on.

Note For definitions of these alarms, see the *Cisco ONS 15327 Troubleshooting Guide*.

Stop. You have completed this procedure.

DLP-B301 Initiate a BLSR Manual Ring Switch

Purpose	This task performs a BLSR Manual ring switch.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Traffic is not protected during a Force protection switch.

Step 1 Display the network view.

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

Step 3 Choose the BLSR and click **Edit**.

Tip To move an icon to a new location, for example, to see BLSR channel (port) information more clearly, click an icon on the Edit BLSR network graphic and while pressing **Ctrl**, drag the icon to a new location.

Step 4 Right-click any BLSR node channel (port) and choose **Set West Protection Operation** (if you chose a west channel) or **Set East Protection Operation** (if you chose an east channel).

Note For two-fiber BLSRs, the squares on the node icons represent the BLSR working and protect channels. You can right-click either channel.

Step 5 In the Set West Protection Operation dialog box or the Set East Protection Operation dialog box, choose **MANUAL RING** from the drop-down menu. Click **OK**.

Step 6 Click **Yes** in the two Confirm BLSR Operation dialog boxes.

Step 7 From the File menu, choose **Close**.

Step 8 Return to your originating procedure (NTP).

DLP-B241 Clear a BLSR Manual Ring Switch

Purpose	This task clears a Manual ring switch.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Traffic is not protected during a Force protection switch.

Step 1 Display the network view.

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

Step 3 Choose the BLSR and click **Edit**.

Tip To move an icon to a new location, for example, to see BLSR channel (port) information more clearly, click an icon on the Edit BLSR network graphic and while pressing **Ctrl**, drag the icon to a new location.

Step 4 Right-click the BLSR node channel (port) where the Manual ring switch was applied and choose **Set West Protection Operation** or **Set East Protection Operation**, as applicable.

Step 5 In the dialog box, choose **CLEAR** from the drop-down menu. Click **OK**.

Step 6 Click **Yes** on the Confirm BLSR Operation dialog box. The letter “M” is removed from the channel (port) and the span turns green.

Step 7 From the File menu, choose **Close**.

Step 8 Return to your originating procedure (NTP).

Add and Remove Nodes

This chapter explains how to add and remove nodes Cisco ONS 15327 nodes from bidirectional line switched rings (BLSRs) and unidirectional path switched rings (UPSRs).

Before You Begin

Before performing any of the following procedures, complete the "NTP-B195 Document Existing Provisioning" procedure on page 6-2. Also investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15327 Troubleshooting Guide* as necessary.

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-B12 Add a BLSR Node, page 13-2—Complete as needed.
2. NTP-B213 Remove a BLSR Node, page 13-9—Complete as needed.
3. NTP-B105 Add a UPSR Node, page 13-13—Complete as needed.
4. NTP-B106 Remove a UPSR Node, page 13-15—Complete as needed.

NTP-B12 Add a BLSR Node

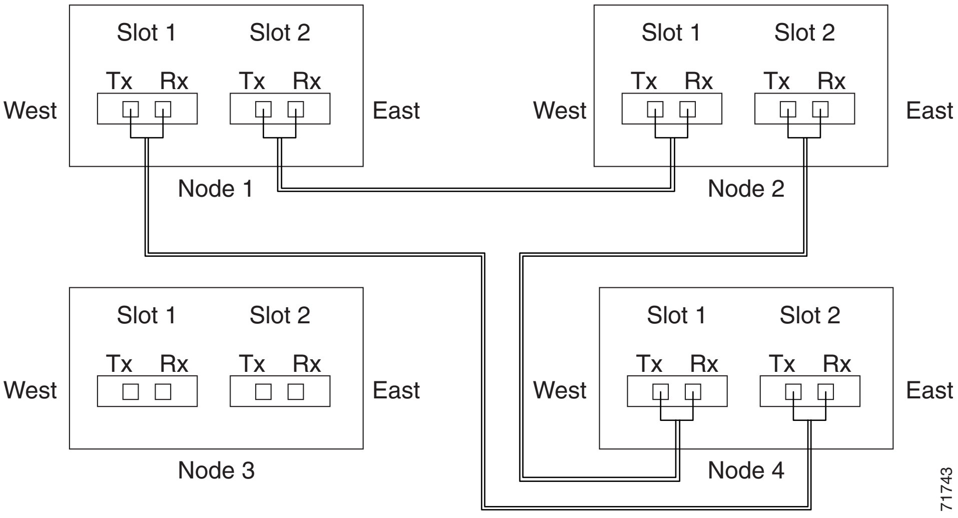
Purpose	This procedure expands a BLSR by adding a node.
Tools/Equipment	Fiber for new node connections
Prerequisite Procedures	Cards must be installed and node turn-up procedures completed on the node that will be added to the BLSR. See Chapter 1, "Install Hardware," and Chapter 3, "Turn Up Node." NTP-B108 Back Up the Database, page 14-6
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Adding a BLSR node can be service affecting and should be performed during a maintenance window.

Note If the node you are adding to the BLSR is not provisioned as an external network element (ENE) is on the same subnet as other BLSR nodes and CTC computers are directly connected to BLSR nodes, you expect a CTC computer will connect to it,

Step 1 Draw a diagram of the BLSR where you will add the node. In the diagram, identify the east and west BLSR OC-N trunk (span) cards that will connect to the new node. This information is essential to complete this procedure without error. Figure 13-1 shows a drawing of a three-node, two-fiber BLSR that uses Slots 1 and 2 for the BLSR trunk cards.

Figure 13-1 Three-Node Two-Fiber BLSR Before a Fourth Node Is Added



Step 2 Verify the card installation on the new node using the "NTP-B24 Verify Card Installation" procedure on page 3-2. Verify that the OC-N cards that will be the BLSR trunk (span) cards match the BLSR optical rate. For example, if the BLSR is OC-48, the new node must have OC-48 cards installed. If the OC-N cards are not installed or the optical rates do not match the BLSR, complete the "NTP-B218 Install the Optical and Ethernet Cards" procedure on page 1-23.

Step 3 Verify that fiber is available to connect the new node to the existing nodes. Refer to the diagram drawn in Step 1.

Step 4 Complete the "NTP-B35 Verify Node Turn Up" procedure on page 4-2. In order to have CTC visibility to the new node after it is added, you must be an authorized user on the node and you must have IP connectivity to the node.

Step 5 Log into a node that is in the BLSR. See the "DLP-B60 Log into CTC" task on page 2-23.

Step 6 Complete the "DLP-B302 Check BLSR or UPSR Alarms and Conditions" task on page 13-5 to verify that the BLSR is free of major alarms or problems. If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See Chapter 6, "Manage Alarms" or, if necessary, refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 7 Click the **Provisioning > BLSR** tabs.

Step 8 On paper, record the Ring ID, Ring Type, Line Rate, and Ring Reversion.

Step 9 From the Node column, record the Node IDs in the BLSR. The Node IDs are the numbers in parentheses next to the node name.

Step 10 Log into the new node:

- If the node has a LAN connection and is displayed on the network map, from the View menu, choose **Go to Other Node**, then choose the new node from the Select Node to Go to pull-down menu on the Select Node dialog box and click **OK**.
- If the new node is not connected to the network, log into it directly using the "DLP-B60 Log into CTC" task on page 2-23.

Step 11 Click the **Alarms** tab. Verify that no critical or major alarms are present, nor any facility alarms, such as LOS, LOF, AIS-L, SF, and SD. If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See Chapter 6, "Manage Alarms"or, if necessary, refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 12 Complete the following steps if the node is on the same subnet as other BLSR nodes, it is not provisioned as an external network element (see "NTP-B169 Set Up CTC Network Access" procedure on page 3-7), and a CTC computer will directly connect to the node while other CTC computers are directly connected to other BLSR nodes. If not, continue with Step 13.

a. Click the **Provisioning > Network > General** tabs. View the IP Address and Net/Subnet Mask Length fields to verify the node is on the same subnet as other BLSR nodes.

b. Click the **Static Route** tab and click **Create**.

c. In the Create Static Route dialog box, enter the following settings:

- Destination IP address: **IP address of CTC computer directly connected to the node**
- Net Mask: **255.255.255.255**
- Next Hop: **IP address of the Cisco ONS 15327**
- Cost: **1**

d. Click **OK**.

Step 13 Using the information recorded in Steps 8 and 9 and the diagram created in Step 1, create a BLSR on the new node. See the "DLP-B242 Create a BLSR on a Single Node" task on page 13-6.

Step 14 (Optional) Create test circuits, making sure they pass through the BLSR trunk cards, and run test traffic through the node to ensure that the cards are functioning properly. See the "NTP-B189 Create a Manually Routed Optical Circuit" procedure on page 5-38 and the "NTP-B62 Test Optical Circuits" procedure on page 5-46 for information.

Step 15 Create the DCC terminations on the new node. See the "DLP-B253 Provision SONET DCC Terminations" task on page 4-4.

Note Creating the DCC terminations causes the SDCC Termination Failure and Loss of Signal alarms to appear. These alarms will remain active until you connect the node to the BLSR.

Note If you map the K3 byte to another byte (such as E2), you must remap the line cards on either side of the new node to the same byte. See the "DLP-A89 Remap the K3 Byte" task on page 5-16.

Step 16 Log into a BLSR node that will connect to the new node using one of the login options in Step 10.

Step 17 Referring to the diagram created in Step 1, complete the "DLP-B303 Initiate a BLSR Force Ring Switch" task on page 13-6 on the node that will connect to the new node via its west port.

Step 18 Referring to the diagram created in Step 1, complete the "DLP-B303 Initiate a BLSR Force Ring Switch" task on page 13-6 on the node that will connect to the new node via its east port.

Step 19 Click the **Alarms** tab. If unexpected critical or major alarms are present, resolve them before you continue. If necessary, refer to the alarm troubleshooting procedures in the *Cisco ONS 15327 Troubleshooting Guide.*

Step 20 Following the diagram created in Step 1, remove the fiber connections from the two nodes that will connect to the new node.

a. Remove the west fiber from the node that will connect to the east port of the new node. In the Figure 13-1 example, this is Node 1/Slot 1

b. Remove the east fiber from the node that will connect to the west port of the new node. In the Figure 13-1 example, this is Node 4/Slot 2.

Step 21 Connect fibers from the adjacent nodes to the new node following the diagram created in Step 1. Connect the west port to the east port and the east port to the west port.

Step 22 Display the newly added node in node view.

Step 23 Click the **Provisioning > BLSR** tabs.

Step 24 Click **Ring Map**. Verify that the new node appears on the Ring Map with the other BLSR nodes, then click **OK**.

Step 25 From the View menu, choose **Go to Network View** and verify the following:

a. Click the **Provisioning > BLSR** tabs. Verify that the new node is displayed under the Node column.

b. Click the **Alarms** tab. Verify that BLSR alarms such as RING MISMATCH, E-W MISMATCH, PRC-DUPID (duplicate node ID), and APSCDFLTK (default K) are not present.

If the new node does not appear in the Node column, or if BLSR alarms are displayed, log into the new node and verify that the BLSR is provisioned on it correctly with the information from Steps 8 and 9. If the node still does not appear, or if alarms persist, refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 26 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 27 In network view, right-click the new node and choose **Update Circuits With The New Node** from the shortcut menu. Verify that the number of updated circuits displayed in the dialog box is correct.

Step 28 If incomplete circuits still appear, refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 29 Click the **History** tab. Verify that BLSR_RESYNC conditions are present for every node in the BLSR.

Step 30 Complete the "DLP-B194 Clear a BLSR Force Ring Switch" task on page 13-8 to remove the ring switch from the east and west BLSR lines.

Step 31 (Optional) Complete the "NTP-B175 BLSR Acceptance Test" procedure on page 4-16.

Stop. You have completed this procedure.

DLP-B302 Check BLSR or UPSR Alarms and Conditions

Purpose	Use this task to check a BLSR or a UPSR for alarms and conditions before performing any major change to the ring such as adding and removing nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 From the View menu choose **Go to Network View**. Verify that all BLSR or UPSR spans on the network map are green.

Step 2 Click the **Alarms** tab. Verify that no critical or major alarms are present, nor any facility alarms, such as LOS, LOF, AIS-L, SF, and SD. In a BLSR, these facility conditions might be reported as minor alarms. Make sure the Filter button in the lower right corner of the window is off (not indented).

Step 3 Click the **Conditions** tab and click **Retrieve Conditions.** Verify that no ring switches are active. Make sure the Filter button in the lower right corner of the window is off (not indented).

Step 4 Return to the originating procedure (NTP).

DLP-B242 Create a BLSR on a Single Node

Purpose	Use this task to create a BLSR on a single node. The task is used when you add a node to an existing BLSR or when you delete and then recreate a BLSR temporarily on one node.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 In node view, lick the **Maintenance > BLSR** tabs.

Step 2 In the Suggestion dialog box, click **OK**.

Step 3 In the Create BLSR dialog box, enter the BLSR information:

- Ring Type—Enter **2 Fiber**. You cannot provision 4-Fiber BLSRs on ONS 15327s.
- Ring ID—Enter the BLSR ring ID. If the node is being added to a BLSR, use the BLSR ring ID.
- Node ID—Enter the node ID. If the node is being added to a BLSR, use an ID that is not used by other BLSR nodes.
- Ring Reversion—Enter the ring reversion time of the existing BLSR.
- West Line—Enter the slot on the node that will connect to the existing BLSR via the node's west line.
- East Line—Enter the slot on the node that will connect to the existing BLSR via the node's east line.

Step 4 Click **OK**.

Note Alarms are displayed and the BLSR is displayed as Incomplete until the node is connected to other BLSR nodes.

Step 5 Return to your originating procedure (NTP).

DLP-B303 Initiate a BLSR Force Ring Switch

Purpose	Use this task to perform a BLSR Force protection operation on a BLSR port.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Traffic is not protected during a Force protection switch.

Note A Force switch request on a span or card causes CTC to raise a FORCED-REQ condition. It is informational only; the condition will clear when the force switch command is cleared.

Step 1 From the View menu, choose **Go to Network View**.

Step 2 the **Provisioning > BLSR** tabs.

Step 3 Click **Edit**.

Step 4 To apply a Force switch to the west line:

a. Right-click the west BLSR port where you want to switch the BLSR traffic and choose **Set West Protection Operation**.

Note If node icons overlap, drag and drop the icons to a new location or return to network view and change the positions of the network node icons, because BLSR node icons are based on the network view node icon positions.

Note For two-fiber BLSRs, the squares on the node icons represent the BLSR working and protect channels. You can right-click either channel. For four-fiber BLSRs, the squares represent ports. Right-click either working port.

b. In the Set West Protection Operation dialog box, choose **FORCE RING** from the pull-down menu. Click **OK**.

c. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

On the network graphic, an F is displayed on the working BLSR channel where you invoked the protection switch. The span lines change color to reflect the forced traffic. Green span lines indicate the new BLSR path, and the lines between the protection switch are purple.

Performing a Force switch generates several conditions including FORCED-REQ-RING, FORCED-REQ-RING, and WKSWPR.

Step 5 To apply a Force switch to the east line:

a. Right-click the east BLSR port and choose **Set East Protection Operation**.

Note If node icons overlap, drag and drop the icons to a new location or return to network view and change the positions of the network node icons, because BLSR node icons are based on the network view node icon positions.

Note The squares on the node icons represent the BLSR working and protect channels. You can right-click either channel.

b. In the Set East Protection Operation dialog box, choose **FORCE RING** from the pull-down menu. Click **OK**.

c. Click **Yes** in the two Confirm BLSR Operation dialog boxes that display.

On the network graphic, an F appears on the working BLSR channel where you invoked the protection switch. The span lines change color to reflect the forced traffic. Green span lines indicate the new BLSR path, and the lines between the protection switch are purple.

Performing a Force switch generates several conditions including FORCED-REQ-RING, FORCED-REQ-RING, and WKSWPR.

Step 6 From the File menu, choose **Close**.

Step 7 Return to your originating procedure (NTP).

DLP-B194 Clear a BLSR Force Ring Switch

Purpose	Use this task to remove a BLSR Force ring switch.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Display the network view.

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

Step 3 Click **Edit**.

Step 4 To clear a Force switch on the west line:

a. Right-click the BLSR west port where you want to clear the protection switch and choose **Set West Protection Operation**. Ports with a Force switch applied are marked with an F.

b. In the Set West Protection Operation dialog box, choose **CLEAR** from the pull-down menu. Click **OK**.

c. In the Confirm BLSR Operation dialog box, click **Yes**.

Step 5 To clear a Force switch on the east line:

a. Right-click the BLSR east port where you want to clear the protection switch and choose **Set East Protection Operation**. Ports with a Force switch applied are marked with an F.

b. In the Set East Protection Operation dialog box, choose **CLEAR** from the pull-down menu. Click **OK**.

c. In the Confirm BLSR Operation dialog box, click **Yes**.

On the BLSR network graphic, a green and a purple span line connects each node. This is the normal display for BLSR spans when a protection switch is not present.

Step 6 From the File menu, choose **Close**.

Step 7 Return to your originating procedure (NTP).

NTP-B213 Remove a BLSR Node

Purpose	This procedure removes a node from a BLSR.
Tools/Equipment	None
Prerequisite Procedures	NTP-B108 Back Up the Database, page 14-6
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution The following procedure minimizes traffic outages during node removals. You will delete all circuits that originate and terminate on the node that will be removed.

Caution If you remove a node that is the only BITS timing source for the ring, you also remove the only source of synchronization for all the nodes in that ring. Circuits that leave the ring to connect to other networks synchronized to a Stratum 1 clock will experience a high level of pointer adjustments, which might adversely affect traffic performance.

Step 1 Log into a node on the BLSR. Do not log into the node that you will remove. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions.

Step 2 Create a diagram of the BLSR where you will remove the node. You can draw the BLSR manually, or print it from CTC by performing the following steps:

a. From the View menu, choose **Go to Network View**.

b. Click the **BLSR** tab, click the BLSR, then click **Edit**.

c. In the BLSR window, verify that all the port information is visible. If not, press **Ctrl** and drag the node icons to a new location so the information can be viewed.

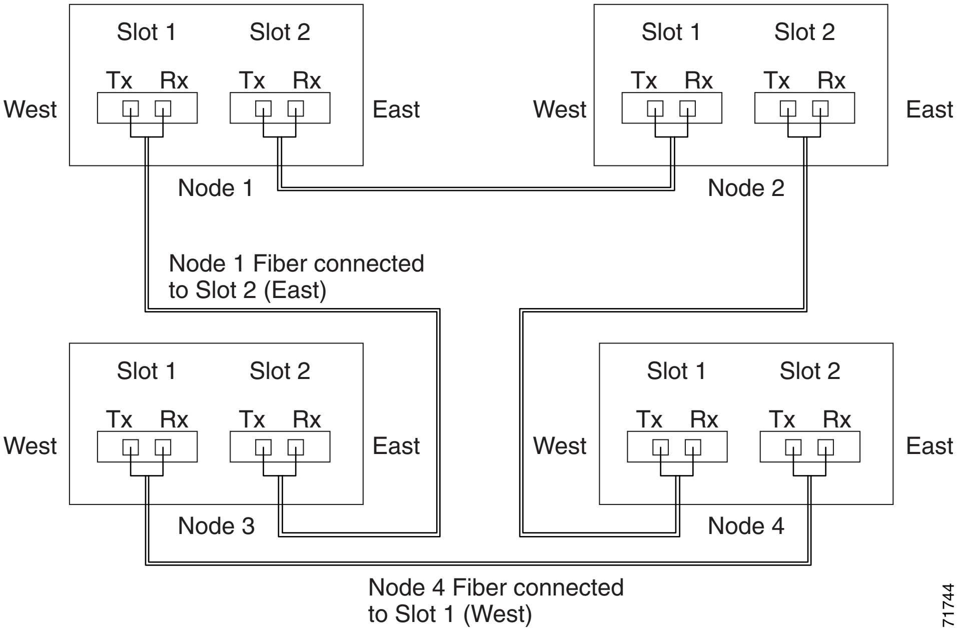
d. From the File menu, choose **Print**.

e. Close the BLSR window by choosing **Close** from the File menu.

Step 3 Referring to the BLSR diagram, identify the following:

- The node that is connected through its west port to the node that will be removed. For example, if you were removing Node 3 in Figure 13-2, Node 1 is the node connected through its west port to Node 3.
- The node that is connected via its east port to the target (removed) node. In Figure 13-2, Node 3 is the node connected via its east port to Node 4.

Figure 13-2 Four-Node, Two-Fiber BLSR Before a Node Is Removed



Step 4 Complete the "DLP-B302 Check BLSR or UPSR Alarms and Conditions" task on page 13-5 to verify that the BLSR is free of alarms. If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See Chapter 6, "Manage Alarms" or, if necessary, refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 5 From the View menu choose **Go to Other Node**. Choose the node that you will remove and click **OK**.

Step 6 Click the **Circuits** tab. If the Scope setting is set to Network, choose **Node** from the Scope pull-down menu. Make sure the Filter button is off (not indented) to ensure that all circuits are visible.

Step 7 Delete all circuits that originate or terminate on the node. See the "NTP-B152 Delete Circuits" procedure on page 8-13.

Step 8 Complete the "DLP-B304 Verify BLSR Pass-Through Circuits" task on page 13-11 to verify that circuits passing through the target node enter and exit the node on the same STS and/or VT.

Step 9 From the View menu choose **Go to Network View**.

Step 10 Referring to the diagram created in Step 1, complete the "DLP-B303 Initiate a BLSR Force Ring Switch" task on page 13-6 at each node that connects to the target node to force traffic away from the target node. You must perform a Force switch at each port connected to the target node. For example, in Figure 13-2, you would perform a Force switch on the east port of Node 4 and the west port of Node 1.

Step 11 Click the **Alarms** tab. If unexpected critical or major alarms are present, resolve them before you continue. If necessary, refer to the alarm troubleshooting procedures in the *Cisco ONS 15327 Troubleshooting Guide.*

Step 12 Remove the fiber connections between the target node and the two neighboring nodes.

Step 13 Reconnect the fiber of the two neighboring nodes directly, west port to east port.

Step 14 On the removed node, complete the "DLP-B196 Delete a BLSR from a Single Node" task on page 13-12 to remove the BLSR from the former BLSR trunk card.

Note If you delete a node that was in a login node group, you will see incomplete circuits for that node in the CTC network view. (Although it is no longer part of the ring, the removed node still reports to CTC until it is no longer in a login node group.)

Step 15 Click the **History** tab. Verify that the BLSR_RESYNC condition is present for every node in the BLSR.

Step 16 Complete the "DLP-B194 Clear a BLSR Force Ring Switch" task on page 13-8 for both switches.

Step 17 Complete the "DLP-B195 Verify Timing in a Reduced Ring" task on page 13-12.

Step 18 (Optional) Complete the "NTP-B175 BLSR Acceptance Test" procedure on page 4-16.

Stop. You have completed this procedure.

DLP-B304 Verify BLSR Pass-Through Circuits

Purpose	Use this task to verify that circuits passing through a node that will be removed from a BLSR enter and exit the node on the same STS and/or VT.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 On the CTC Circuits window, choose a circuit that passes through the target BLSR node and click **Edit**.

Step 2 In the Edit Circuits window, check **Show Detailed Map**.

Step 3 Verify that the STS and VT mapping on the node's east and west ports are the same. For example, if a circuit mapping on the west port s5/p1/S1 (Slot 5, Port 1, STS 1), verify that the mapping is STS 1 on the east port. If the circuit displays different STSs and/or VTs on the east and west ports, write down the name of the circuit.

Step 4 Repeat Steps 1 through 3 for each circuit displayed in the Circuits tab.

Delete and recreate each circuit recorded in Step 3 that entered/exited the node on different STSs. To delete the circuit, complete the "NTP-B152 Delete Circuits" procedure on page 8-13. To create circuits, complete the appropriate procedures in Chapter 5, "Create Circuits and VT Tunnels."

Step 5 Return to your originating procedure (NTP).

DLP-B195 Verify Timing in a Reduced Ring

Purpose	Use this task to verify timing in the ring where you removed a node.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 Identify the type of timing (Line, External, Mixed) in the Timing Mode field.

Step 3 Scroll down to the Reference Lists and observe the NE Reference fields to see the timing references provisioned for that node.

Step 4 If the removed node was the only BITS timing source, perform the following:

a. Look for another node on the ring that can be used as a BITS source and set that node's Timing Mode to **External**. Choose that node as the primary timing source for all other nodes in the ring. See the "DLP-B157 Change the Node Timing Source" task on page 10-15.

b. If no node in the reduced ring can be used as a BITS source, choose one node to be your internal timing source. Set that node's Timing Mode to **External**, set the BITS 1 and 2 State field to **OOS**, and set the NE Reference to **Internal Clock**. Then, choose line timing for all other nodes in the ring. This forces the first node to be their primary timing source. See the "DLP-B157 Change the Node Timing Source" task on page 10-15.

Note Internal timing conforms to Stratum 3 requirements and is not considered optimal.

Step 5 If the removed node was not the only BITS timing source, provision the adjacent nodes to line timing using SONET links (east and west) as timing sources, traceable to the node with external BITS timing. See the "NTP-B28 Set Up Timing" procedure on page 3-16.

Step 6 Return to your originating procedure (NTP).

DLP-B196 Delete a BLSR from a Single Node

Purpose	Use this task to delete a BLSR from a node after you remove the node from the BLSR.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, display the node that was removed from the BLSR.

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

Step 3 Highlight the ring and click **Delete**.

Step 4 In the Suggestion dialog box, click **OK**.

Step 5 In the confirmation message, confirm that this is the ring you want to delete. If so, click **Yes**.

Step 6 Return to your originating procedure (NTP).

NTP-B105 Add a UPSR Node

Purpose	This procedure adds a node to a UPSR.
Tools/Equipment	None
Prerequisite Procedures	Cards must be installed and node turnup procedures completed on the node that will be added to the UPSR. See Chapter 1, "Install Hardware," and Chapter 3, "Turn Up Node." NTP-B108 Back Up the Database, page 14-6
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Step 1 Verify the card installation on the new node. See the "NTP-B24 Verify Card Installation" procedure on page 3-2.

Step 2 Verify that the OC-N cards that will serve as the UPSR trunk (span) cards match the UPSR optical rate of the trunk cards to which the new node will be connected. For example, if the adjacent nodes have OC-48 line cards, the new node must have OC-48 cards installed. If the OC-N cards are not installed or the rate does not match the rate of the adjacent node trunk cards, complete the "NTP-B218 Install the Optical and Ethernet Cards" procedure on page 1-23 to install them.

Step 3 Verify that fiber is available to connect the new node to the existing nodes.

Step 4 Complete the "NTP-B35 Verify Node Turn Up" procedure on page 4-2.

Step 5 Log into a node in the UPSR where you want to add a node. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions. In order to have CTC visibility to the new node after it is added, you must be an authorized user on the node and you must have IP connectivity to the node.

Step 6 Complete the "DLP-B302 Check BLSR or UPSR Alarms and Conditions" task on page 13-5 to verify that the UPSR is free of major alarms or problems. If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See Chapter 6, "Manage Alarms" or, if necessary, refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 7 Log into the new node:

- If the node has a LAN connection and is displayed on the network map, from the View menu, choose **Go to Other Node**, then choose the new node from the Select Node to Go to pull-down menu on the Select Node dialog box and click **OK**.
- If the new node is not connected to the network, log into it directly using the "DLP-B60 Log into CTC" task on page 2-23.

Step 8 Click the **Alarms** tab. Verify that no critical or major alarms are present, nor any facility alarms, such as LOS, LOF, AIS-L, SF, and SD. If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See Chapter 6, "Manage Alarms"or, if necessary, refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 9 Complete the following steps if the node is on the same subnet as other BLSR nodes, it is not provisioned as an external network element (see "NTP-B169 Set Up CTC Network Access" procedure on page 3-7), and a CTC computer will directly connect to the node while other CTC computers are directly connected to other BLSR nodes. If not, continue with Step 10.

a. Click the **Provisioning > Network > General** tabs. View the IP Address and Net/Subnet Mask Length fields to verify the node is on the same subnet as other BLSR nodes.

b. Click the **Static Route** tab and click **Create**.

c. In the Create Static Route dialog box, enter the following settings:

- Destination IP address: **IP address of CTC computer directly connected to the node**
- Net Mask: **255.255.255.255**
- Next Hop: **IP address of the Cisco ONS 15327**
- Cost: **1**

d. Click **OK**.

Step 10 (Optional) Create test circuits, making sure they pass through the UPSR line cards, and run test traffic through the node to ensure the cards are functioning properly. See the "NTP-B189 Create a Manually Routed Optical Circuit" procedure on page 5-38 and the "NTP-B62 Test Optical Circuits" procedure on page 5-46 for information.

Step 11 Create the DCC terminations on the new node. See the "DLP-B253 Provision SONET DCC Terminations" task on page 4-4.

Step 12 From the View menu, choose **Go to Network View**.

Step 13 Complete the "DLP-B197 Initiate a UPSR Force Switch" task on page 13-16 to switch traffic away from the span that will be broken to connect to the new node.

Caution Traffic is not protected during a protection switch.

Step 14 Two nodes will connect directly to the new node; remove their fiber connections:

a. Remove the east fiber connection from the node that will connect to the west port of the new node.

b. Remove the west fiber connection from the node that will connect to the east port of the new node.

Step 15 Replace the removed fibers with the fibers that are connected to the new node.

Step 16 Log out of CTC and log back into a node in the network.

Step 17 From the View menu, choose **Go to Network View** to display the UPSR nodes. The new node should appear in the network map. Wait for a few minutes to allow all the nodes to appear.

Step 18 Click the **Circuits** tab and wait for all the circuits to appear, including spans. Count the number of incomplete circuits.

Step 19 In the network view, right-click the new node and choose **Update Circuits With New Node** from the list of options. Wait for the confirmation dialog box to appear. Verify that the number of updated circuits in the dialog box is correct.

Step 20 Click the **Circuits** tab and verify that no incomplete circuits are displayed.

Step 21 Complete the "DLP-B198 Clear a UPSR Switch" task on page 13-17.

Step 22 (Optional) Complete the "NTP-B177 UPSR Acceptance Test" procedure on page 4-23.

Stop. You have completed this procedure.

NTP-B106 Remove a UPSR Node

Purpose	This procedure removes a node from a UPSR.
Tools/Equipment	None
Prerequisite Procedures	NTP-B108 Back Up the Database, page 14-6
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution The following procedure minimizes traffic outages during node removals.

Caution If you remove a node that is the only BITS timing source for the ring, you also remove the only source of synchronization for all the nodes in that ring. Circuits that connect to other networks which are synchronized to a Stratum 1 clock will experience a high level of pointer adjustments, which might adversely affect customer service.

Step 1 Draw a diagram of the UPSR where you will remove the node. In the diagram, identify the following:

- The node that is connected through its west port to the node that will be removed (the target node).
- The node that is connected through its east port to the target node.

Step 2 Log into a node in the network where you want to remove a UPSR node. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions.

Step 3 Complete the "DLP-B302 Check BLSR or UPSR Alarms and Conditions" task on page 13-5 to verify that the UPSR is free of alarms. If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See Chapter 6, "Manage Alarms" or, if necessary, refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 4 Complete the "NTP-B152 Delete Circuits" procedure on page 8-13 for circuits that originate or terminate in the target node. (If a circuit has multiple drops, delete only the drops that terminate on the node you are deleting.)

Step 5 Complete the "DLP-B197 Initiate a UPSR Force Switch" task on page 13-16 for all spans connected to the node you are removing.

Caution Traffic is not protected during a forced protection switch.

Step 6 Remove all fiber connections between the target node and the two neighboring nodes.

Step 7 Reconnect the fiber of the two neighboring nodes directly, west port to east port.

> **Note** If you delete a node that was in a login node group, you will see incomplete circuits for that node in CTC network view. (Although it is no longer part of the ring, the removed node still reports to CTC until it is no longer in a login node group.)

Step 8 Exit CTC and log back in. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions.

Step 9 Log into each newly-connected node and open the **Alarms** tab. Verify that the trunk cards are free of alarms. Resolve any alarms before proceeding. Refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Step 10 Complete the "DLP-B195 Verify Timing in a Reduced Ring" task on page 13-12.

Step 11 Complete the "DLP-B198 Clear a UPSR Switch" task on page 13-17.

Step 12 Click the **Circuits** tab and verify that no incomplete circuits are present.

Step 13 (Optional) Complete the "NTP-B177 UPSR Acceptance Test" procedure on page 4-23.

Stop. You have completed this procedure.

DLP-B197 Initiate a UPSR Force Switch

Purpose	Use this task to switch all circuits on a UPSR span to another span.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

> **Caution** Traffic is not protected during Force UPSR switches.

Step 1 From the View menu choose **Go to Network View**.

Step 2 Right-click the span where you want to Force switch UPSR traffic. Choose **Circuits** from the shortcut menu.

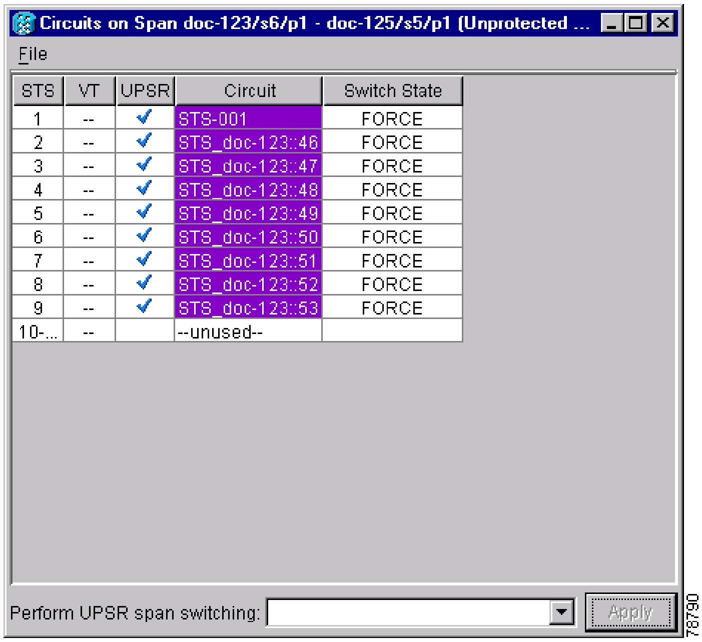
Step 3 In the Circuits on Span dialog box, choose **FORCE SWITCH AWAY**. Click **Apply**.

Step 4 In the Confirm UPSR Switch dialog box, click **Yes**.

Step 5 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span window, the Switch State for all circuits is Force. Figure 13-3 shows an example.

Figure 13-3 Circuits on Span Dialog Box with a Force Switch


Circuits on Span doc-123/s6/p1 - doc-125/s5/p1 (Unprotected ...
File
Perform UPSR span switching:
Apply
78790

STS	VT	UPSR	Circuit	Switch State
1	--	✓	STS-001	FORCE
2	--	✓	STS_doc-123::46	FORCE
3	--	✓	STS_doc-123::47	FORCE
4	--	✓	STS_doc-123::48	FORCE
5	--	✓	STS_doc-123::49	FORCE
6	--	✓	STS_doc-123::50	FORCE
7	--	✓	STS_doc-123::51	FORCE
8	--	✓	STS_doc-123::52	FORCE
9	--	✓	STS_doc-123::53	FORCE
10-...	--		--unused--	

Note A Force switch request on a span or card causes CTC to raise a FORCED-REQ condition. The condition clears when you clear the Force switch; it is informational only.

Step 6 Return to your originating procedure (NTP).

DLP-B198 Clear a UPSR Switch

Purpose	Use this task to clear a UPSR Force switch.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Right-click the span where you want to clear the switch. Choose **Circuits** from the shortcut menu.

Step 3 In the Circuits on Span dialog box, choose **CLEAR** to remove the switch. Click **Apply**.

Step 4 In the Confirm UPSR Switch dialog box, click **Yes**.

Step 5 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span window, the Switch State for all UPSR circuits is CLEAR.

Step 6 Return to your originating procedure (NTP).

Maintain the Node

This chapter provides procedures for maintaining the Cisco ONS 15327.

Before You Begin

Before performing any of the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15327 Troubleshooting Guide* as necessary. This section lists the chapter procedures (NTPs). Turn to a procedure to view its tasks (DLPs).

1. NTP-B107 Inspect and Maintain the Air Filter, page 14-2—Complete as needed.
2. NTP-B108 Back Up the Database, page 14-6—Complete as needed.
3. NTP-B109 Restore the Database, page 14-8—Complete as needed.
4. NTP-B163 Restore the Node to Factory Configuration, page 14-10—Complete as needed to clear the database and upload a blank database and the latest software.
5. NTP-B214 Offload the Security Audit Trail Log, page 14-15—Complete as needed.
6. NTP-B110 Inhibit Protection Switching, page 14-16—Complete as needed.
7. NTP-B111 Revert to an Earlier Software Load, page 14-19—Complete as needed.
8. NTP-B112 Clean Fiber Connectors, page 14-20—Complete as needed.
9. NTP-B113 Reset the XTC Using CTC, page 14-23—Complete this procedure as needed to reset the XTC card and switch the node to the redundant XTC.
10. NTP-B215 View G1000-2 Ethernet Maintenance Information, page 14-24—Complete as needed.
11. NTP-B228 View E10/100-4 Ethernet Maintenance Information, page 14-25--Complete as needed.
12. NTP-B225 Switch the Node Timing Reference, page 14-27—Complete this procedure as needed to switch the node timing reference to perform maintenance or return to normal timing operation.

NTP-B107 Inspect and Maintain the Air Filter

Purpose	This procedure explains how to inspect and maintain reusable and disposable air filters.
Tools/Equipment	Spare air filters
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Retrieve or higher

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

Note Although the filter works if it is installed with either side facing left, Cisco recommends that you install it with the metal bracing facing left to preserve the surface of the filter.

Step 1 As needed, complete the "DLP-B 199 Inspect, Clean, and Replace the Reusable Air Filter" task on page 14-2.

Step 2 As needed, complete the "DLP-B 200 Inspect and Replace the Disposable Air Filter" task on page 14-4.

Stop. You have completed this procedure.

DLP-B199 Inspect, Clean, and Replace the Reusable Air Filter

Purpose	This task ensures that the air filter is free from dirt and dust, which allows optimum air flow and prevents dirt and dust from entering the shelf.
Tools/Equipment	Vacuum or detergent Water faucet Spare filter Pinned hex key tool
Prerequisite Procedures	None
Required/As Needed	Inspection required every 30 days. Clean as needed.
Onsite/Remote	Onsite
Security Level	Retrieve or higher

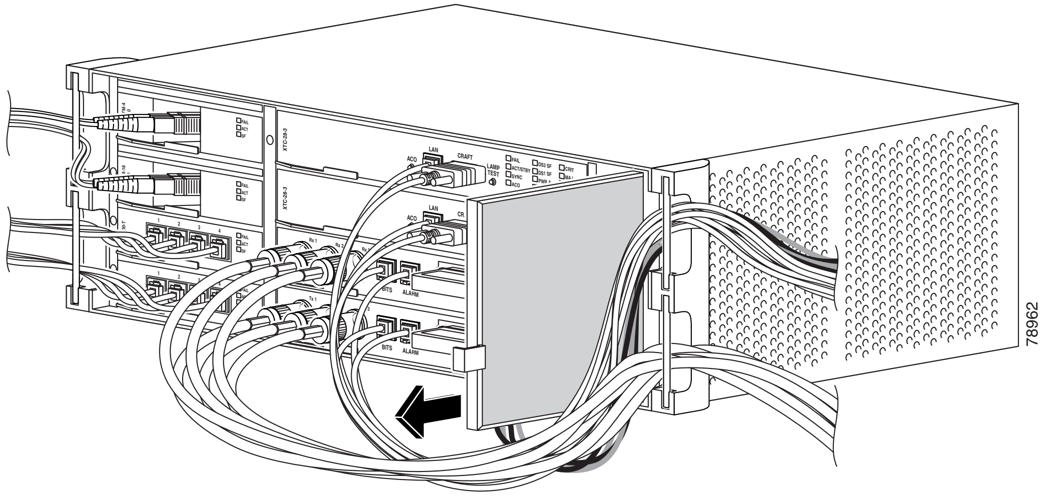
Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.**

Step 1 Verify that you are replacing a 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 15327 use a reusable air filter.

Step 2 Move any cables that are routed in front of the fan-tray assembly and air filter so you can easily slide the filter out (Figure 14-1).

Step 3 Grasp the metal tab at the edge of the filter and slide the filter out of the bracket while being careful not to dislodge any dust that might have collected on the filter.

Figure 14-1 Removing the Reusable Fan-Tray Air Filter



Step 4 Visually inspect the filter material for dirt and dust.

Step 5 If the reusable air filter contains a concentration of dirt and dust, either vacuum or wash the air filter. Prior to washing the air filter, replace the dirty air filter with a spare clean air filter (spare filters should be kept in stock).

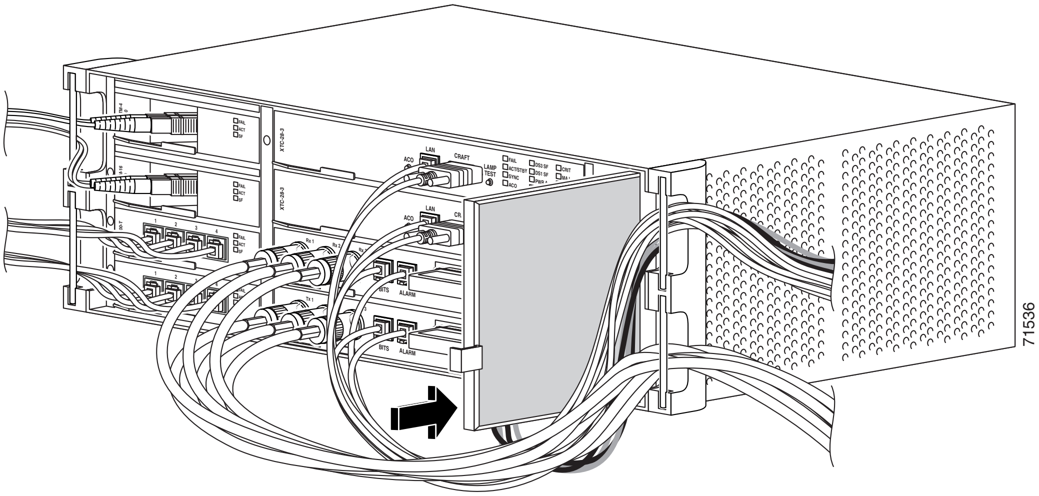
Step 6 Wash the dirty air filter under a faucet with a light detergent. After washing the air filter, allow it to completely air dry for at least eight hours before reusing.

Note Cleaning should take place outside the operating environment to avoid releasing dirt and dust near the equipment.

Warning **Do not put a damp filter back in the ONS 15327.**

Step 7 Slide the clean air filter back into the shelf (Figure 14-2).

Figure 14-2 Replacing the Reusable Fan-Tray Air Filter



Step 8 Return to your originating procedure (NTP).

DLP-B200 Inspect and Replace the Disposable Air Filter

Purpose	This task ensures that the air filter is free from dirt and dust to allow optimum air flow and prevent dirt and dust from entering the ONS 15327.
Tools/Equipment	Extra filters Pinned hex key
Prerequisite Procedures	None
Required/As Needed	Inspection required every 30 days. Replace as needed.
Onsite/Remote	Onsite
Security Level	Retrieve or higher

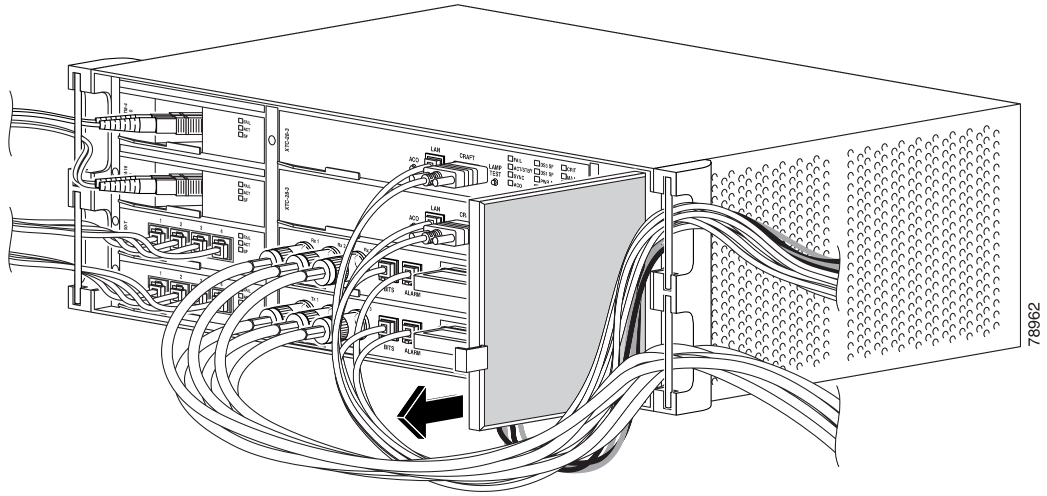
Note The disposable air filter is installed to the right of the fan-tray assembly only, so you must remove the assembly to inspect and replace the disposable air filter.

Step 1 Verify that you are replacing a disposable air filter. The disposable filter is made of spun white polyester that is flame retardant. NEBS 3E and earlier versions of the ONS 15327 use a disposable air filter.

Step 2 Move any cables that are routed in front of the fan-tray assembly and air filter so you can easily slide the filter out (Figure 14-3).

Step 3 Grasp the metal tab at the edge of the filter and slide the filter out of the bracket while being careful not to dislodge any dust that might have collected on the filter.

Figure 14-3 Removing the Disposable Fan-Tray Air Filter

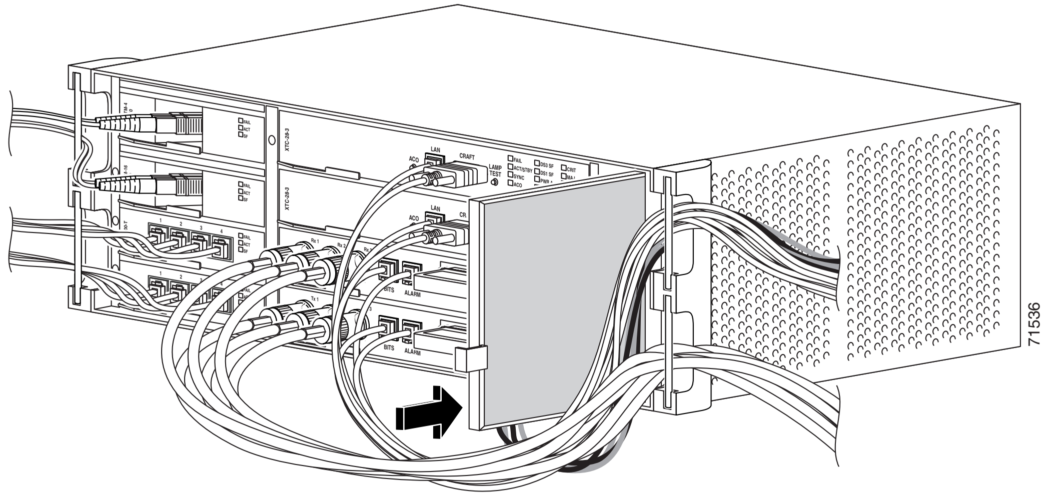


Step 4 Visually inspect the filter material for dirt and dust.

Step 5 If the disposable air filter shows a heavy concentration of dirt and dust, replace it with a new filter.

Step 6 Slide the new air filter back into the shelf (Figure 14-4).

Figure 14-4 Replacing the Disposable Fan-Tray Air Filter



Step 7 Return to your originating procedure (NTP).

NTP-B108 Back Up the Database

Purpose	This procedure stores a backup version of the XTC (software) database on the workstation running CTC or on a network server.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	Required. Cisco recommends performing a database backup at approximately weekly intervals and prior to and after configuration changes.
Onsite/Remote	Onsite or remote
Security Level	Superuser

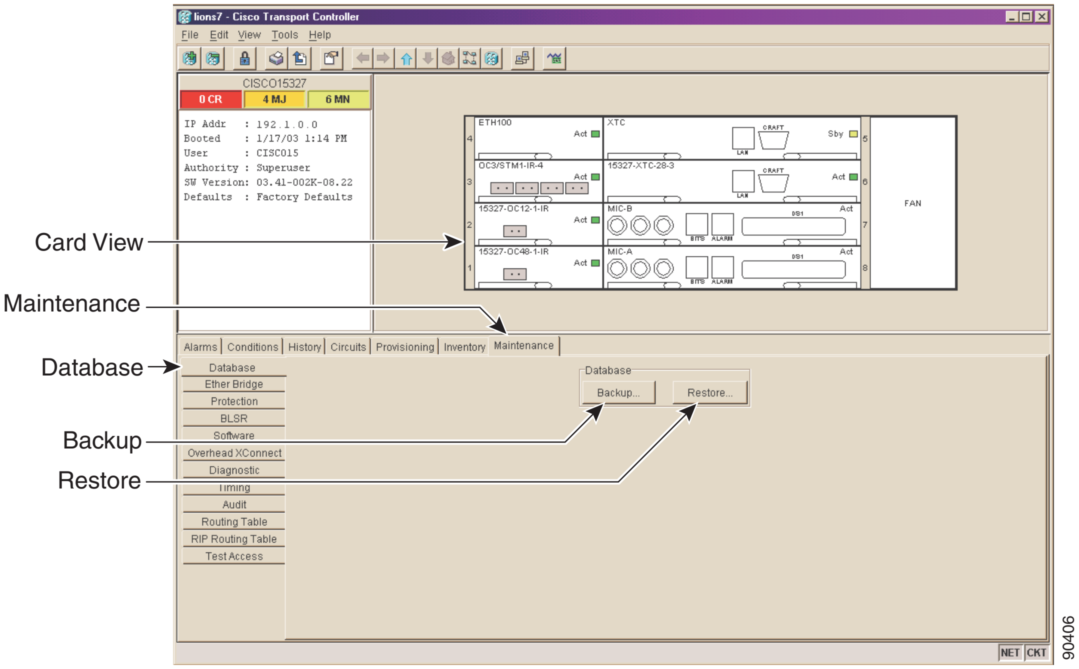
Note You must back up and restore the database for each node on a circuit path in order to maintain a complete circuit.

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

Step 1 Complete the "DLP-B 60 Log into CTC" task on page 2-23 at the node where you will perform the database backup. If you are already logged in, continue with Step 2.

Step 2 In node (default) view, click the **Maintenance > Database** tabs (Figure 14-5).

Figure 14-5 Backing Up the XTC Database



```
IP Addr    : 192.1.0.0
Booted     : 1/17/03 1:14 PM
User       : CISCO15
Authority  : Superuser
SW Version: 03.41-002K-08.22
Defaults   : Factory Defaults
```

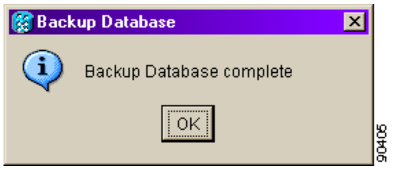
Step 3 Click **Backup**.

Step 4 Save the database on the workstation's hard drive or on network storage. Use an appropriate file name with the .db file extension; for example, database.db.

Step 5 Click **Save**.

Step 6 Click **OK** in the confirmation dialog box (Figure 14-6).

Figure 14-6 Confirming the Database Backup



Backup Database complete

Stop. You have completed this procedure.

NTP-B109 Restore the Database

Purpose	This procedure restores the software database.
Tools/Equipment	None
Prerequisite Procedures	NTP-B108 Back Up the Database, page 14-6
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

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

Caution G1000-2 cards lose traffic for approximately 90 seconds when an ONS 15327 database is restored. Traffic is lost during the period of spanning tree reconvergence. The CARLOSS alarm appears and clears during this period.

Caution If you are restoring the database on multiple nodes, wait until the XTC reboot has completed on each node before proceeding to the next node.

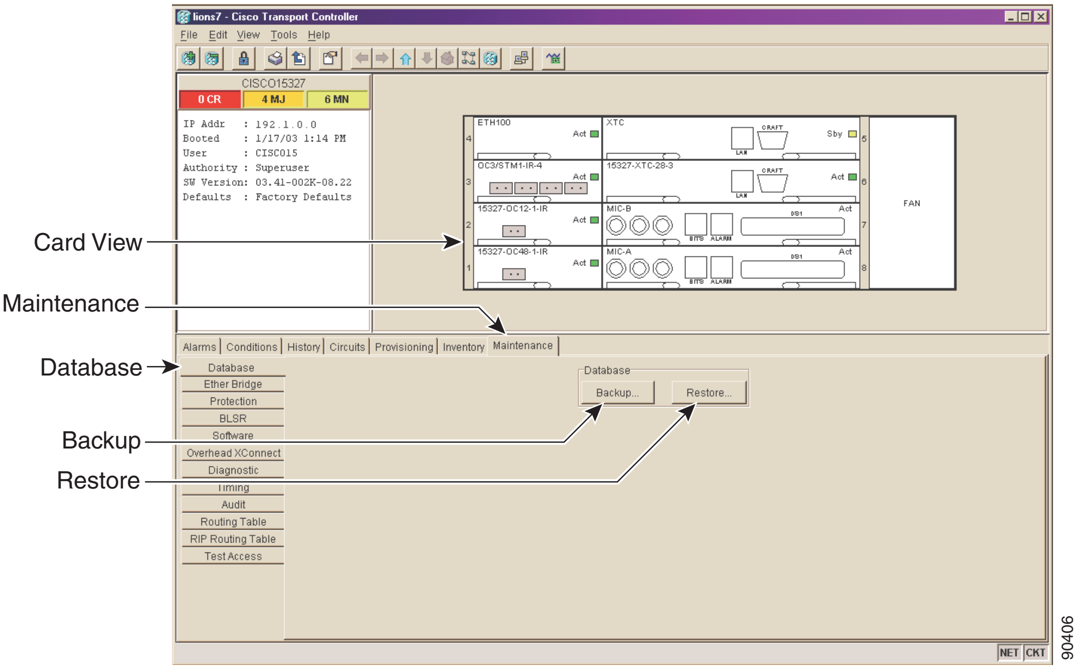
Step 1 Complete the "DLP-B 60 Log into CTC" task on page 2-23 at the node where you will restore the database. If you are already logged in, proceed to Step 2.

Step 2 If there are switch events that need to be cleared, in node (default) view, click the **Maintenance > BLSR** tabs and view the West Switch and East Switch columns.

- **a.** If there is a switch event (not caused by a line failure), clear the switch by choosing **CLEAR** from the drop-down menu and click **Apply**.
- **b.** If there is a switch event caused by the Wait to Restore (WTR) condition, choose **LOCKOUT SPAN** from the drop-down menu and click **Apply**. When the LOCKOUT SPAN is applied, choose **CLEAR** from the drop-down menu and click **Apply**.

Step 3 In node view, click the **Maintenance > Database** tabs (Figure 14-7).

Figure 14-7 Restoring the XTC Database



```
IP Addr   : 192.1.0.0
Booted    : 1/17/03 1:14 PM
User      : CISCO15
Authority : Superuser
SW Version: 03.41-002K-08.22
Defaults  : Factory Defaults
```

Step 4 Click **Restore**.

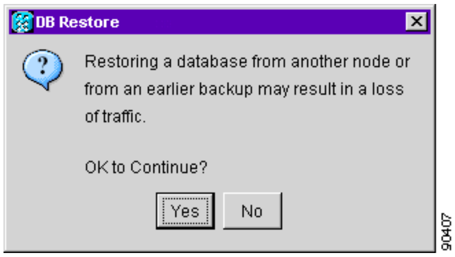
Step 5 Locate the database file stored on the workstation's hard drive or on network storage.

Note To clear all existing provisioning, locate and upload the database found on the latest ONS 15327 software CD.

Step 6 Click the database file to highlight it.

Step 7 Click **Open**. The DB Restore dialog box appears. Opening a restore file from another node or from an earlier backup might affect traffic on the login node (Figure 14-8).

Figure 14-8 Restoring the Database—Traffic Loss Warning



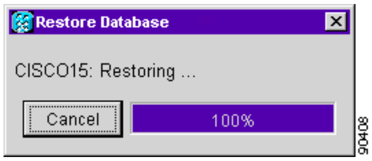
Restoring a database from another node or from an earlier backup may result in a loss of traffic.

OK to Continue?

Step 8 Click **Yes** in the DB Restore dialog box.

The Restore Database dialog box monitors the file transfer (Figure 14-9).

Figure 14-9 Restoring the Database—In-Process Notification



Restore Database

CISCO15: Restoring ...

Step 9 Wait for the file to complete the transfer to the XTC.

Step 10 Click **OK** when the "Lost connection to node, changing to Network View" dialog box appears. Wait for the node to reconnect.

Step 11 If you cleared a switch in Step 2, reapply the switch as needed.

Stop. You have completed this procedure.

NTP-B163 Restore the Node to Factory Configuration

Purpose	This procedure clears the XTC database and restores customer or factory defaults. This process involves uploading the most recent software package and a blank database. This process is performed by the RE-INIT.jar utility, also called the reinitialization tool.
Tools/Equipment	Software CD containing Release 3.4 software, the node's NE defaults, and the reinitialization tool. JRE 1.03_02 must also be installed on the computer you will use to perform this procedure.
Prerequisite Procedures	NTP-B108 Back Up the Database, page 14-6
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser

Caution If you are restoring the database on multiple nodes, wait until the XTC cards have rebooted on each node before proceeding to the next node.

Caution Cisco strongly recommends that you keep different node databases in separate folders. This is because the reinitialization tool will choose the first product-specific software package in the specified directory if you only use the Search Path field. You might accidentally copy an incorrect database if multiple databases are kept in the specified directory.

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

Step 1 If you need to install or replace one or more XTC cards, see the "NTP-B 217 Install the XTCs" procedure on page 1-21.

Step 2 If you are using Microsoft Windows, complete the "DLP-B 244 Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)" task on page 14-11.

Step 3 If you are using UNIX, complete the "DLP-B 245 Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)" task on page 14-13.

Stop. You have completed this procedure.

DLP-B244 Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)

Purpose	This task describes how to use the reinitialization tool in Windows. Use this tool to clear the database on the XTC, upload software, and restore factory or customer defaults.
Tools/Equipment	Software CD containing Release 3.4 software, the NE defaults, and the reinitialization tool JRE 1.03_02 must also be installed on the computer you use to perform this procedure. Straight-through (Category 5) LAN cable
Prerequisite Procedures	NTP-B108 Back Up the Database, page 14-6
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser

Note The XTC cards reboot several times during this procedure. Wait until they are completely rebooted before continuing.

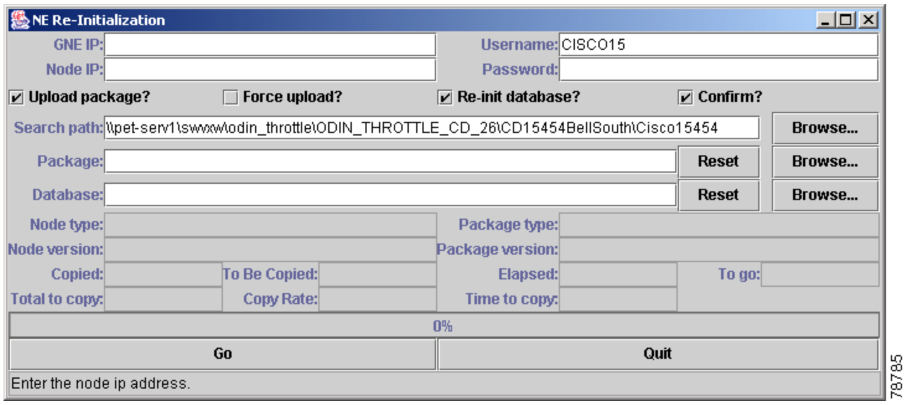
Step 1 Insert the system software CD containing the reinitialization tool, the CTC software, and the defaults database into the local craft interface PC drive. If the CTC Installation Wizard opens, click **Cancel**.

Step 2 To find the recovery tool file, go to **Start > Run > Browse** and select the CD drive.

Step 3 On the CD drive, go to the CISCO15327 folder and set the Files of Type drop-down menu to **All Files**.

Step 4 Select the **RE-INIT.jar** file and click **Open** to open the reinitialization tool (Figure 14-10).

Figure 14-10 Reinitialization Tool in Windows



NE Re-Initialization

GNE IP:
Node IP:
Username: CISCO15
Password:

☑ Upload package? □ Force upload? ☑ Re-init database? ☑ Confirm?

Search path: \\pet-serv1\swxw\odin_throttle\ODIN_THROTTLE_CD_26\CD15454BellSouth\Cisco15454

Package:
Database:

0%

Enter the node ip address.

Step 5 If the node you are reinitializing is an external network element (ENE) in a proxy server network, enter the IP address of the gateway network element (GNE) in the GNE IP field. If not, leave it blank.

Step 6 Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 14-10).

Step 7 Verify that the Re-Init Database, Upload Package, and Confirm check boxes are checked. If one is not checked, click the check box.

Step 8 In the Search Path field, verify that the path to the CISCO15327 folder on the CD drive is listed.

Caution Cisco strongly recommends that you keep different node databases in separate folders. This is because the reinitialization tool will choose the first product-specific software package in the specified directory if you use the Search Path field instead of the Package and Database fields. You might accidentally copy an incorrect database if multiple databases are kept in the specified directory.

Caution Before you perform the next step, be sure you are uploading the correct database. You cannot reverse the upload process after you click Yes.

Step 9 Click **Go**.

Step 10 A confirmation dialog box opens (Figure 14-11). Click **Yes**.

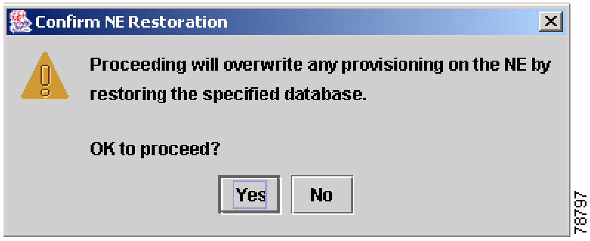
Step 11 The status bar at the bottom of the screen displays Complete when the node has activated the software and uploaded the database.

Note The Complete message only indicates that the XTC successfully uploaded the database, not that the database restore was successful. The XTC then tries to restore the database after it reboots.

Step 12 If you are logged into CTC, close the browser window and disconnect the straight-through LAN cable from the RJ-45 (LAN) port on the XTC or on the hub or switch to which the ONS 15327 is physically connected. Reconnect your straight-through LAN cable to the LAN port and log back into CTC. See the "NTP-B 22 Set Up CTC Computer to Connect to the ONS 15327" procedure on page 2-8.

Step 13 Manually set the node name and network configuration to site-specific values. See the "NTP-B 25 Set Up Name, Date, Time, and Contact Information" procedure on page 3-5 and "NTP-B 169 Set Up CTC Network Access" procedure on page 3-7 for information on setting the node name, IP address, mask and gateway, and IIOP port.

Figure 14-11 Confirm NE Restoration



Confirm NE Restoration

Proceeding will overwrite any provisioning on the NE by restoring the specified database.

OK to proceed?

Step 14 Return to your originating procedure (NTP).

DLP-B245 Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)

Purpose	This task describes how to use the reinitialization tool in a UNIX environment. Use this tool to clear the database on the XTC and restore factory or customer defaults.
Tools/Equipment	Software CD containing Release 3.4 software, the node's NE defaults, and the reinitialization tool. JRE 1.03_02 must also be installed on the computer you will use to perform this procedure.
Prerequisite Procedures	NTP-B108 Back Up the Database, page 14-6
Required/As Needed	As needed to clear the existing database from an XTC and restore the node's default settings.
Onsite/Remote	Onsite or remote
Security Level	Superuser

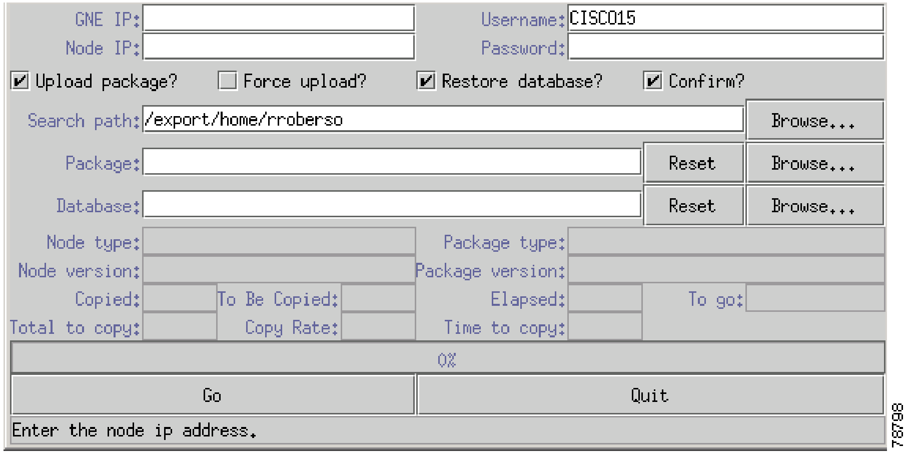
Note The XTC cards will reboot several times during this procedure. Wait until they are completely rebooted before continuing.

Step 1 Insert the system software CD containing the reinitialization tool, the software, and the defaults database into the local craft interface PC drive. If the CTC Installation Wizard opens, click **Cancel**.

Step 2 To find the recovery tool file, go to the CISCO15327 directory on the CD (usually /cdrom/cdrom0/CISCO15327).

Step 3 If you are using a file explorer, double click the **RE-INIT.jar** file to open the reinitialization tool (Figure 14-12 on page 14-14). If you are working with a command line interface, run **`java -jar RE-INIT.jar`**.

Figure 14-12 Reinitialization Tool in UNIX



GNE IP:
Node IP:
Username: CISCO15
Password:

☑ Upload package? □ Force upload? ☑ Restore database? ☑ Confirm?

Search path: /export/home/rroberso
Package:
Database:
Node type:
Node version:
Package type:
Package version:
Copied:
To Be Copied:
Elapsed:
To go:
Total to copy:
Copy Rate:
Time to copy:

0%

Enter the node ip address.

Step 4 If the node you are reinitializing is an external network element (ENE) in a proxy server network, enter the IP address of the gateway network element (GNE) in the GNE IP field. If not, leave it blank.

Step 5 Enter the node name or IP address of the node you are reinitializing in the Node IP field (Figure 14-12).

Step 6 Verify that the Re-Init Database, Upload Package, and Confirm check boxes are checked. If any are not checked, click that check box.

Step 7 In the Search Path field, verify that the path to the CISCO15327 folder on the CD drive is listed.

Caution Cisco strongly recommends that you keep different node databases in separate folders. This is because the reinitialization tool will choose the first product-specific software package in the specified directory if you use the Search Path field instead of the Package and Database fields. You might accidentally copy an incorrect database if multiple databases are kept in the specified directory.

Caution Before you perform the next step, be sure you are uploading the correct database. You cannot reverse the upload process after you click Yes.

Step 8 Click **Go**.

Step 9 A confirmation dialog box opens (Figure 14-11 on page 14-13). Click **Yes.**

Step 10 The status bar at the bottom of the screen displays Complete when the node has activated the software and uploaded the database.

Note The Complete message only indicates that the XTC successfully uploaded the database, not that the database restore was successful. The XTC then tries to restore the database after it reboots.

Step 11 If you are logged into CTC, close the browser window and disconnect the straight-through LAN cable from the RJ-45 (LAN) port on the XTC or on the hub or switch to which the ONS 15327 is physically connected. Reconnect your straight-through LAN cable to the LAN port and log back into CTC. See the "DLP-B 53 Set Up a Solaris Workstation for a Craft Connection to an ONS 15327" task on page 2-17.

Step 12 Manually set the node name and network configuration to site-specific values. See the "NTP-B 25 Set Up Name, Date, Time, and Contact Information" procedure on page 3-5 and "NTP-B 169 Set Up CTC Network Access" procedure on page 3-7 for information on setting the node name, IP address, mask and gateway, and IIOP port.

Step 13 Return to your originating procedure (NTP).

NTP-B214 Offload the Security Audit Trail Log

Purpose	This procedure stores up to 650 audit trail log entries in a local or network drive file to maintain a record of actions performed for the node.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed. If the audit trail log is not offloaded, the oldest entries will be overwritten after the log reaches capacity.
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Complete the "DLP-B 60 Log into CTC" task on page 2-23 at the node where you will offload the audit trail log. If you are already logged in, proceed to Step 2.

Step 2 In the node view, click the **Maintenance > Audit** tabs.

Step 3 Click **Retrieve**.

Step 4 Click **Archive**.

Step 5 In the Archive Audit Trail dialog, navigate to the directory (local or network) where you want to save the file.

Step 6 Enter a name in the File Name field.

You do not have to give the archive file a particular extension. It is readable in any application that supports text files, such as WordPad, Microsoft Word (imported), etc.

Step 7 Click **Save**.

Up to 640 entries will be saved in this file. The next entries will continue with the next number in the sequence, rather than starting over.

Note Once you have archived a group of audit trail entries, they are no longer visible in CTC. The entries cannot be imported into CTC.

Stop. You have completed this procedure.

NTP-B110 Inhibit Protection Switching

Purpose	This procedure describes how to apply and remove a lock on or lock out on a traffic card in a protection configuration. For bidirectional line switch ring (BLSR) span lockouts, see the "DLP-B 301 Initiate a BLSR Manual Ring Switch" task on page 12-9 and the "DLP-B 241 Clear a BLSR Manual Ring Switch" task on page 12-10.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser

Step 1 To prevent traffic on a working or protect card from switching to the other card in the pair, complete the "DLP-B 201 Apply a Lock On" task on page 14-16.

Step 2 To switch traffic from a working or protect card to the other card in the pair to prevent revertive switching, complete the "DLP-B 202 Apply a Lock Out" task on page 14-17.

Note A combination of lock on and lock out is allowed in 1:1 and 1:N protection; for example, a lock on on the working card and a lock out on the protect card are permissible.

Step 3 To remove a lock on or lock out and return a protection group to its usual switching method, complete the "DLP-B 203 Clear a Lock On or Lock Out" task on page 14-18.

Note A non-alarmed event (INHSW) is raised when a card is placed in a lock on or lock out state.

Note Refer to the *Cisco ONS 15327 Reference Manual* for a description of protection switching and switch state priorities.

Stop. You have completed this procedure.

DLP-B201 Apply a Lock On

Purpose	This task prevents traffic from being switched from one card to another.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance

Note To apply a lock on to a protect card in a 1:1 protection group, the protect card must be active. If the protect card is in standby, the Lock On button is disabled. To make the protect card active, you must switch traffic from the working card to the protect card (Step 4). When the protect card is active, you can apply the lock on.

Step 1 Use the following rules to determine if you can put the intended card in a lock on state:

- For a 1:1 electrical protection group, both the working and protect cards can be placed in the lock on state.
- For a 1+1 optical protection group, only the working card can be placed in the lock on state.

Step 2 In node view, click the **Maintenance > Protection** tabs.

Step 3 Under Protection Groups, click the protection group where you want to apply a lock on.

Step 4 If you determine that the protect card is in standby and you want to apply the lock on to the protect card, make the protect card active:

a. Under Selected Group, click the protect card.

b. Under Switch Commands, click **Switch**.

Step 5 Under Selected Group, click the active card where you want to lock traffic.

Step 6 From Inhibit Switching, click **Lock On**.

Step 7 Click **Yes** in the confirmation dialog box.

The lock on has been applied and traffic cannot be switched to the working card. To clear the lock on, see the "DLP-B 203 Clear a Lock On or Lock Out" task on page 14-18.

Step 8 Return to your originating procedure (NTP).

DLP-B202 Apply a Lock Out

Purpose	This task switches traffic from one card to another using a lock out, which is a switching mechanism that overrides other manual switching connections (Force, Manual, and Exercise).
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance

Note Multiple lock outs in the same protection group are not allowed.

Step 1 Use the following rules to determine if you can put the card in a lock out state:

- For a 1:1 electrical protection group, both the working and protect cards can be placed in the lock out state.
- For a 1+1 optical protection group, only the protect card can be placed in the lock out state.

Step 2 In node view, click the **Maintenance > Protection** tabs.

Step 3 Under Protection Groups, click the protection group that contains the card you want to lock out.

Step 4 Under Selected Group, click the card you want to lock traffic out of.

Step 5 From Inhibit Switching, click **Lock Out**.

Step 6 Click **Yes** in the confirmation dialog box.

The lock out has been applied and traffic is switched to the opposite card. To clear the lock out, see the "DLP-B 203 Clear a Lock On or Lock Out" task on page 14-18.

Note Provisioning a lock out causes a LOCKOUT-REQ or an FE-LOCKOUT condition to be raised on CTC. Clearing the lockout switch request clears these conditions; they are informational only.

Step 7 Return to your originating procedure (NTP).

DLP-B203 Clear a Lock On or Lock Out

Purpose	This task clears a lock on or lock out.
Tools/Equipment	None
Prerequisite Procedures	DLP-B201 Apply a Lock On, page 14-16 or DLP-B202 Apply a Lock Out, page 14-17
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 Under Protection Groups, click the protection group that contains the card you want to clear.

Step 3 Under Selected Group, click the card you want to clear.

Step 4 From Inhibit Switching, click **Unlock**.

Step 5 Click **Yes** in the confirmation dialog box.

The lock on or lock out is cleared.

Step 6 Return to your originating procedure (NTP).

NTP-B111 Revert to an Earlier Software Load

Purpose	This procedure reverts the ONS 15327 database to an earlier software load. Reverting to a R3.3.0 or later load will switch to the older software load and its database without affecting traffic or DCC connectivity.
Tools/Equipment	This feature requires dual XTC cards
Prerequisite Procedures	This feature requires Software R3.3.0 or later as the protect version.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

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

Note Provisioning performed after a software load is activated (upgraded to a higher software release) will not reinstate with a revert. The database configuration at the time of activation is reinstated by a revert. This note does not apply to maintenance reverts (for example, 2.2.2 to 2.2.1), because maintenance releases use the same database (a revert to a maintenance release software load will use the current active database; therefore, no provisioning is lost).

Step 1 Complete the "DLP-B 60 Log into CTC" task on page 2-23 at the node where you will perform the revert. If you are already logged in, go to Step 2.

Step 2 Record the IP address of that node. The address can be obtained using one of the following methods:

- The IP address is displayed on the left side in node view.
- In node (default) view, click the **Provisioning > Network > General** tabs.

Step 3 If reverting to a previous software release (not a maintenance release), record any new circuits created since the previous software upgrade. These circuits will have to be manually recreated (if needed) after the software reversion has taken place.

Step 4 Click the **Maintenance > Software** tabs.

Step 5 Verify that the protect software is Software R3.3.0 or later. If the protect software is not Software R3.3.0 or later, do not revert.

Step 6 Click **Revert**. The Revert button activates the protect software load.

Step 7 Click **Yes** in the revert confirmation dialog box. The ONS 15327 reboots and loses the connection to CTC.

Step 8 Wait until the software upgrade finishes. This might take as long as 30 minutes.

Step 9 When the software upgrade is finished, click the **Delete CTC Cache** button in the browser window.

Step 10 Close the browser.

Step 11 Restart the browser and log back into the node using the IP address recorded in Step 2. See the "DLP-B 60 Log into CTC" task on page 2-23 as necessary.

The browser downloads the CTC applet for the standby software load.

Step 12 If needed, recreate the circuits recorded in Step 3. See Chapter 5, "Create Circuits and VT Tunnels" for specific circuit creation procedures.

Stop. You have completed this procedure.

NTP-B112 Clean Fiber Connectors

Purpose	This procedure cleans the fiber connectors.
Tools/Equipment	Inspection microscope Compressed air/duster Type A Fiber Optic Connector Cleaner (CLETOP reel) Isopropyl alcohol 70 percent or higher Optical swab Optical receiver cleaning stick
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Maintenance

Warning **Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam or view directly with optical instruments.**

Step 1 Using an inspection microscope, inspect each fiber connector for dirt, cracks, or scratches.

Step 2 Replace any damaged fiber connectors.

Note Replace all dust caps whenever the equipment will not be immediately used.

Step 3 Complete the "DLP-B 204 Scope and Clean Fiber Connectors and Adapters with Alcohol and Dry Wipes" task on page 14-21 as necessary.

Step 4 Complete the "DLP-B 205 Clean Fiber Connectors with CLETOP" task on page 14-21 as necessary.

Step 5 Complete the "DLP-B 206 Clean the Fiber Adapters" task on page 14-22 as necessary.

Caution Do not reuse the optical swabs. Keep unused swabs off of work surfaces.

Stop. You have completed this procedure.

DLP-B204 Scope and Clean Fiber Connectors and Adapters with Alcohol and Dry Wipes

Purpose	This task cleans the fiber connectors and adapters with alcohol and dry wipes.
Tools/Equipment	Compressed air/duster Isopropyl alcohol, 70 percent or higher Optical swab Optical receiver cleaning stick
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Maintenance

Warning **Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam or view directly with optical instruments.**

Step 1 Remove the dust cap from the fiber connector.

Step 2 Wipe the connector tip with the pre-moistened alcohol wipe.

Step 3 Blow dry using filtered air.

Step 4 Use an inspection microscope to inspect each fiber connector for dirt, cracks, or scratches. If the connector is not clean, repeat Steps 1 through 3.

Step 5 Insert the fiber connector into the applicable adapter or attach a dust cap to the fiber connector.

Note If you must replace a dust cap on a connector, first verify that the dust cap is clean. To clean the dust cap, wipe the outside of the cap using a dry lint free wipe and the inside of the dust cap using a CLETOP stick swab (14100400).

Step 6 Return to your originating procedure (NTP).

DLP-B205 Clean Fiber Connectors with CLETOP

Purpose	This task cleans the fiber connectors with CLETOP.
Tools/Equipment	Type A fiber optic connector cleaner (CLETOP reel) Optical receiver cleaning stick
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Maintenance

Step 1 Remove the dust cap from the fiber connector.

Step 2 Press the lever down to open the shutter door. Each time you press the lever, you expose a clean wiping surface.

Step 3 Insert the connector into the CLETOP cleaning cassette slot, rotate one quarter turn, and gently swipe downwards.

Step 4 Use an inspection microscope to inspect each fiber connector for dirt, cracks, or scratches. If the connector is not clean, repeat Steps 1 through 3.

Step 5 Insert the fiber connector into the applicable adapter or attach a dust cap to the fiber connector.

Note If you must replace a dust cap on a connector, first verify that the dust cap is clean. To clean the dust cap, wipe the outside of the cap using a dry lint free wipe and the inside of the dust cap using a CLETOP stick swab (14100400).

Step 6 Return to your originating procedure (NTP).

DLP-B206 Clean the Fiber Adapters

Purpose	This task cleans the fiber adapters.
Tools/Equipment	CLETOP stick swab
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Maintenance

Step 1 Remove the dust plug from the fiber adapter.

Step 2 Insert a CLETOP stick swab (14100400) into the adapter opening and rotate the swab.

Step 3 Place dust plugs on the fiber adapters when not in use.

Step 4 Return to your originating procedure (NTP).

NTP-B113 Reset the XTC Using CTC

Purpose	This procedure resets the XTC card and switches the node to the redundant XTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

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

Note Before you reset the XTC, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

Note A software or card pull reset of an active XTC card causes a standard Telcordia protection switch of less than 50 ms.

Step 1 Complete the "DLP-B 60 Log into CTC" task on page 2-23 at the node where you will perform the software reset. If you are already logged in, go to Step 2.

Step 2 Right-click the XTC card to reveal a drop-down menu.

Step 3 Click **Reset Card**.

Step 4 Click **Yes** when the "Are You Sure?" dialog box appears.

Step 5 Click **OK** when the "Lost connection to node, changing to Network View" dialog box appears.

Note For LED behavior during an XTC reboot, see "NTP-B 217 Install the XTCs" procedure on page 1-21.

Step 6 Confirm that the XTC you reset is in standby mode after the reset. The information can be obtained using one of the following methods:

- The XTC card's LED will be amber for standby or green for active.
- In node view, run the mouse over the XTC card. A popup box displays whether the card is active or standby.

Stop. You have completed this procedure.

NTP-B215 View G1000-2 Ethernet Maintenance Information

Purpose	This procedure enables viewing the maintenance information on a selected G1000-2 Ethernet card.
Tools/Equipment	None
Prerequisite Procedures	Before you view performance monitoring (PM) values, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 5, "Create Circuits and VT Tunnels" and Chapter 9, "Change Port Settings."
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the "DLP-B 60 Log into CTC" task on page 2-23 at the node that you want to monitor. If you are already logged in, continue with Step 2.

Step 2 As needed, use the following tasks to change the display of Ethernet maintenance information:

- "DLP-B 306 View Loopback Status" task on page 14-24
- "DLP-B 307 View Ethernet Bandwidth Usage" task on page 14-25

Stop. You have completed this procedure.

DLP-B306 View Loopback Status

Purpose	This task changes the screen view to display the loopback status on a selected G1000-2 Ethernet card port.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click a G1000-2 Ethernet card. The card view displays.

Step 2 Click the **Maintenance** tab.

Step 3 Click the **Loopback** tab.

The # and State columns identify the port number and current operating state (IS, OOS, OOS_MT) of each port on the card. The Loopback Type column identifies the type of loopback (None or Terminal) applied to each port on the card.

Step 4 Return to your originating procedure (NTP).

DLP-B307 View Ethernet Bandwidth Usage

Purpose	This task changes the screen view to display Ethernet bandwidth usage on a selected G1000-2 Ethernet card.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click a G1000-2 Ethernet card. The card view displays.

Step 2 Click the **Maintenance** tab.

Step 3 Click the **Bandwidth** tab.

The current STS bandwidth usage information appears.

Step 4 Return to your originating procedure (NTP).

NTP-B228 View E10/100-4 Ethernet Maintenance Information

Purpose	This procedure enables viewing the maintenance information on a selected E10/100-4 Ethernet card.
Tools/Equipment	None
Prerequisite Procedures	Before you view PM values, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see Chapter 5, “Create Circuits and VT Tunnels” and Chapter 9, “Change Port Settings.”
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Complete the “DLP-B 60 Log into CTC” task on page 2-23 at the node that you want to monitor.

Step 2 To view Ethernet spanning tree parameters, click the **Maintenance** > **Ether Bridge** > **Spanning Trees** tabs. The current spanning tree information is displayed.

Step 3 As needed, complete the following tasks:

- DLP-B309 View Ethernet MAC Address Table, page 14-26
- DLP-B310 View Ethernet Trunk Utilization, page 14-26

Stop. You have completed this procedure.

DLP-B309 View Ethernet MAC Address Table

Purpose	This task displays the Ethernet MAC address table for any node with one or more E10/100-4 Ethernet cards installed.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, click the **Maintenance** > **Ether Bridge** > **MAC Table** tabs.

Step 2 Select the appropriate E10/100-4 Ethernet card in the Layer 2 Domain field.

Step 3 Click the **Retrieve** button.

The MAC address table information is displayed.

Step 4 Return to your originating procedure (NTP).

DLP-B310 View Ethernet Trunk Utilization

Purpose	This task displays the Ethernet Trunk bandwidth usage on any node with one or more E10/100-4 Ethernet cards installed.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite ore remote
Security Level	Retrieve or higher

Step 1 In node view, click the **Maintenance** tab > **Ether Bridge** > **Trunk Utilization** tabs.

Step 2 Select the desired time interval in the Interval field.

Step 3 Click the **Refresh** button.

The trunk utilization information for the current and previous time intervals is displayed.

Step 4 Return to your originating procedure (NTP).

NTP-B225 Switch the Node Timing Reference

Purpose	This procedure switches the node timing reference to enable maintenance on a timing reference or to return the node timing to normal operation.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Step 1 Complete the "DLP-B 60 Log into CTC" task on page 2-23 at the node you want to monitor. If you are already logged in, continue with Step 2.

Step 2 As needed, use the following tasks to change the display of Ethernet maintenance information:

- "DLP-B 330 Manual or Force Switch the Node Timing Reference" task on page 14-27
- "DLP-B 331 Clear a Manual or Force Switched Node Timing Reference" task on page 14-28

Stop. You have completed this procedure.

DLP-B330 Manual or Force Switch the Node Timing Reference

Purpose	This task commands the node to switch to the timing reference you have selected, as long as the synchronization status message (SSM) quality of the reference is not less than the reference that the node is currently running.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Step 1 In node view, click the **Maintenance** > **Timing** tabs. The Timing Source window appears.

Step 2 Click the Reference drop-down menu for the desired Clock, and choose the desired reference.

Step 3 Click the Operation drop-down menu for the desired Clock, and choose one of the following options:

- Manual—This operation commands the NE to switch to the reference you have selected, as long as the SSM quality of the reference is not less the reference than the node is currently running.
- Force—This operation commands the NE to switch to the reference you have selected, regardless of the SSM quality, as long as the reference is valid.

Step 4 Click the **Apply** button.

Step 5 Click **Yes** in the confirmation dialog.

- If the selected timing reference is invalid, a warning dialog appears. Click **OK**, and the NE remains on the original timing reference without performing the switch.
- If the selected timing reference is an acceptable valid reference, the NE switches to the selected timing reference.

Step 6 Return to your originating procedure (NTP).

DLP-B331 Clear a Manual or Force Switched Node Timing Reference

Purpose	This task clears a manual or forced node timing reference switch that is currently in place so that timing will go back to normal timing as defined by your system configuration.
Tools/Equipment	None
Prerequisite Procedures	DLP-B60 Log into CTC, page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Step 1 In node view, click the **Maintenance** > **Timing** tabs. The Timing Source window appears.

Step 2 Find the Clock reference that is currently set to Manual or Force in the Operation menu.

Step 3 Click the Operation drop-down menu for the desired Clock, and choose **Clear**.

Step 4 Click the **Apply** button.

Step 5 Click **Yes** in the confirmation dialog.

- If the normal timing reference is invalid or has failed, a warning dialog appears. Click **OK**, and the NE remains on the previous timing reference without performing the switch.
- If the normal timing reference is an acceptable valid reference, the NE switches back to the normal timing reference as defined by the system configuration.

Step 6 Return to your originating procedure (NTP).

CHAPTER 15

Power Down the Node

This chapter explains how to power down a Cisco ONS 15327 node and stop all node activity.

NTP-B114 Power Down the ONS 15327

Purpose	This procedure stops all node activity.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	For software steps the Provisioning level or higher is required. For hardware steps any level is allowed.

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

Caution The following procedure is designed to minimize traffic outages when powering down nodes, but traffic will be lost if you delete and recreate circuits that passed through a working node.

Caution Always use the supplied ESD wristband when working with the Cisco ONS 15327. Plug the wristband into the ESD jack located on the fan-tray assembly or on the lower right outside edge of the shelf on the NEBS 3 shelf assembly. To access the ESD plug on the NEBS 3 shelf assembly, open the front door of the Cisco ONS 15327. The front door is grounded to prevent electrical shock.

Step 1 Identify the node that you want to power down. If no cards are installed, go to Step 12. If cards are installed, log into the node. See the "DLP-B60 Log into CTC" task on page 2-23 for instructions.

Step 2 In network view, verify that the node is not connected to a network.

a. If the node is part of a working network, log out of the node and complete the "NTP-B213 Remove a BLSR Node" procedure on page 13-9 or the "NTP-B106 Remove a UPSR Node" procedure on page 13-15.

Note If the node is in a linear ADM configuration, Step 4 will delete the topology.

Continue with Step 3.

b. If the node is not connected to a working network and the current configurations are no longer required, proceed to Step 3.

Note Current configurations will be saved if Steps 3 through 12 are skipped.

Step 3 In node view, click the **Circuits** tab and verify that no circuits are displayed, then proceed to Step 4. If circuits are displayed, delete all the circuits that originate or terminate in the node, as follows:

a. Click the circuits that need to be deleted and click **Delete**.

b. Click **Yes**.

Repeat until no circuits are displayed.

Step 4 Complete the "NTP-B203 Modify or Delete 1+1 Card Protection Settings" procedure on page 10-12 to delete any optical protection group. You cannot delete the default electrical protection group, XTCPROTGRP.

Repeat until all protection groups are deleted.

Step 5 Complete the "NTP-B204 Delete a SONET DCC Termination" procedure on page 10-14 for all cards. Repeat until no SDCC Terminations appear.

Step 6 Complete the "DLP-B230 Change a Circuit State" task on page 8-7 to change all ports in each card to Out of Service (OOS).

Step 7 Remove all fiber connections to the cards.

Step 8 Complete the "DLP-B320 Delete a Card" task on page 1-26 for all traffic cards. You cannot delete an XTC card.

Step 9 Click **Yes**.

Step 10 After you have deleted the card, open the card ejectors and remove it from the node.

Step 11 Open the ejectors and remove the XTC card from the node. Repeat for the second XTC.

Step 12 Shut off the power from the power supply that feeds the node.

Step 13 Disconnect the node from its external fuse source.

Step 14 Store all the cards you removed and update inventory records according to local site practice.

Stop. You have completed this procedure.

APPENDIX A

CTC Information and Shortcuts

This appendix describes how to navigate within Cisco Transport Controller (CTC) and change the display of CTC table data for the Cisco ONS 15327. It also lists menu and tool options and describes the shelf inventory data presented in CTC. For further information about CTC, refer to the *Cisco ONS 15327 Reference Manual*.

Displaying Node, Card, and Network Views

The Cisco Transport Controller provides three views of the ONS 15327 and ONS network:

- Node view appears when you first log into an ONS 15327. This view shows a graphic of the ONS 15327 shelf and provides access to tabs and subtabs that you use to manage the node.
- Card view provides access to individual ONS 15327 cards. This view provides a graphic of the card and access to tabs and subtabs that you use to manage the card.
- Network view shows all the nodes in a ring. Users can customize the network view, including changing the background color and map. This view provides access to tabs and subtabs that you use to manage the network.

Table A-1 lists different actions for changing CTC views.

Table A-1 Change CTC Views

To display:	Perform one of the following:
Node view	• Log into a node; node view is the default view. • In network view, double-click a node icon or right-click the node and choose **Open Node** from the shortcut menu. • In network view, click a node icon and then choose **Go to Selected Object** from the View menu. • From the CTC View menu, choose **Go to Other Node** and then choose the node you want from the shortcut menu. • Use the arrows on the CTC toolbar to navigate up or down. For example, in network view, click a node and then click the down arrow.

Table A-1 Change CTC Views (continued)

To display:	Perform one of the following:
Network view	• In node view, click the up arrow or the Network View tool on the CTC toolbar. • From the View menu, choose **Go To Network View**.
Card view	• In node view, double-click a card or right-click the card and choose **Open Card**. • In node view, single-click a card icon, then choose **Go to Selected Object** from the View menu. • Use the arrows on the CTC toolbar to navigate up or down. For example, in node view click a card and then click the down arrow.

Manage the CTC Window

Different navigational methods are available within the CTC window to access views and tasks. You can double-click and right-click objects in the graphic area and move the mouse over nodes, cards, and ports to view popup status information.

CTC Menu and Toolbar Options

The CTC window menu bar and toolbar provide primary CTC functions. Table A-2 shows the actions that are available from the CTC menu and toolbar.

Table A-2 CTC Menu and Toolbar Options

Menu	Menu Option	Toolbar	Description
File	Add Node	➕	Adds a node to the current session. See the "DLP-B62 Add a Node to the Current Session or Login Group" task on page 2-26.
	Lock CTC	🔒	Locks CTC without closing the CTC session. A user name and password are required to open CTC.
	Print	🖨	Prints CTC data. See the "DLP-B138 Print CTC Data" task on page 6-2.
	Export	📤	Exports CTC data. See the "DLP-B139 Export CTC Data" task on page 6-3.
	Exit	⇢	Closes the CTC session. The exit icon appears only in the File menu.

Table A-2 CTC Menu and Toolbar Options (continued)

Menu	Menu Option	Toolbar	Description
Edit	Preferences		Displays the Preferences dialog box: General tab—Allows you to change event defaults and manage preferences. Login Node Groups tab—Allows you to create login node groups. See the "DLP-B61 Create Login Node Groups" task on page 2-25. Map tab—Allows you to customize the network view. See the "DLP-B145 Change the Network View Background Color" task on page 10-8 and the "DLP-B268 Apply a Custom Network View Background Map" task on page 10-9. Circuit tab—Allows you to change the color of circuit spans. See the "DLP-B232 Change Active and Standby Span Color" task on page 8-9. Firewall tab—Sets the IIOP listener ports for access to the ONS 15327 through a firewall. See the "NTP-B27 Set Up the ONS 15327 for Firewall Access" procedure on page 3-13.
View	Go to Previous View	⇦	Displays the previous CTC view.
	Go to Next View	⇨	Displays the next CTC view. Available only after you navigate to a previous view. Go to Previous and Go to Next are similar to forward and backward navigation in a web browser.
	Go to Parent View	⇧	References the CTC view hierarchy: network view, node view, and card view. In card view, this command displays the node view; in node view, the command displays network view. Not available in network view.
	Go to Selected Object View	⇩	Displays the object selected in the CTC window.
	Go to Home View		Displays the login node in node view.
	Go to Network View		Displays the network view.
	Go to Other Node		Displays a dialog box allowing you to choose the node name of a network node that you want to view.
	Show Status Bar	—	Click this item to display or hide the status bar at the bottom of the CTC window.
	Show Tool Bar	—	Click this item to display or hide the CTC toolbar.
—	—		Decreases the size of the map area in network view (toolbar only).
—	—		Increases the size of the map area in network view (toolbar only).
—	—		Increases the size of a selected area of the map in network view (toolbar only).

Table A-2 CTC Menu and Toolbar Options (continued)

Menu	Menu Option	Toolbar	Description
Tools	Circuits	—	Displays the following options: • Repair Circuits—(This option is for the Cisco ONS 15454) Repairs incomplete circuits following replacement of the ONS 15454 AIP board. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for more information. • Set Path Selector Attributes—Allows you to edit UPSR circuit path selector attributes. See the "DLP-B233 Edit UPSR Circuit Path Selectors" task on page 8-10. • Set Circuit State—Allows you to change a circuit state. See the "DLP-B230 Change a Circuit State" task on page 8-7. • Convert CTC Circuits to TL1 Cross Connects—If a cross-connect in a circuit gets deleted, this menu option allows a user to repair a circuit by separating an incomplete CTC circuit into TL1 cross-connects. Then, the user can replace the missing cross-connect. See the "NTP-B417 Upgrade TL1 Cross-Connects to CTC Circuits" procedure on page 8-13. • Upgrade TL1 Cross Connects to CTC Circuits—Allows you to convert TL1 cross-connects to CTC circuits. See the "NTP-B416 Convert a CTC Circuit to TL1 Cross-Connects" procedure on page 8-11. • Roll Circuit—Allows you to reroute live traffic without interrupting service. **Note** This feature requires an ONS 15600 on your network. Refer to the *Cisco ONS 15600 Procedure Guide*.
	Manage VLANs	—	Displays a list of VLANs that have been created and allows you to delete or create new VLANs. See Chapter 5, "Create Circuits and VT Tunnels."
	Open TL1 Connection		Displays the TL1 session dialog box so you can create a TL1 session to a specific node. Refer to the *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide*.
	Open IOS Connection		(Cisco ONS 15454 only) Displays the IOS command line interface dialog box if an IOS capable card (ML1000-2 or ML100T-12) is installed in the node. Refer to the *Cisco ONS 15454 ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide*.
Help	Contents and Index	—	Displays the online help window.
	Manage Help	—	Displays the versions of online help loaded on your computer.
	About CTC	—	Displays the software version and the nodes in the CTC session.

CTC Mouse Options

In addition to the CTC menu bar and toolbar, you can invoke actions by double-clicking CTC window items with your mouse, or by right-clicking an item and selecting actions from shortcut menus. Table A-3 lists the CTC window mouse shortcuts.

Table A-3 CTC Window Mouse Shortcuts

Technique	Description
Double-click	• Node in network view—Displays the node view • Card in node view—Displays the card view • Alarm/Event—Displays the alarm or event raising object. • Circuits—Displays the Edit Circuit window.
Right-click	• Network view graphic area—Displays a menu that you can use to create a new domain, change the position and zoom level of the graphic image, save the map layout if you have a Superuser security level, reset the default layout of network view, and set, change, or remove the background image and color. • Node in network view—Displays a menu that you can use to open the node, reset the node icon position to the longitude and latitude set on the Provisioning > General tab, delete the node, fix the node position for auto layout, provision circuits, or update circuits with a new node. • Span in network view—Displays a menu that you can use to view information about the span source and destination ports, the protection scheme, and the optical or electrical level. You can display the Circuits on Spans dialog box, which displays additional span information and allows you to perform UPSR protection switching. You also perform span upgrades from this menu. • Card in node view—Displays a menu that you can use to open, delete, reset, and change cards. The card that you select determines the commands that appear. • Card in card view—Displays a menu that you can use to reset the card or go to the parent view (node view). • Empty slot in node view—Displays a menu with cards that you can select to pre-provision the slot.
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) bandwidth and protection information. • Over card in node view—Displays card type and card status. • Over card port in node view—Displays card name, port state, and alarm profile status. • Over card port in card view—Displays port state, protection status (if applicable), and alarm profile status.

Node View Shortcuts

Table A-4 shows actions you can perform by moving your mouse over the CTC window.

Table A-4 Performing Node View Card Shortcuts

Action	Shortcut
Display card information	Move your mouse over cards in the graphic to display tooltips with the card type, card present or card provisioned but not present, the highest level of alarm (if any), and the alarm profile used by the card.
Open, reset, or delete a card	Right-click a card. Choose **Open** to display the card in card view, **Delete** to delete it, or **Reset** to reset the card. See also the "DLP-B320 Delete a Card" task on page 1-26.
Pre-provision a slot	In node view, right-click an empty slot. Choose the card type that you want to provision in the slot from the shortcut menu. See also the "NTP-B115 Preprovision a Slot" procedure on page 1-28.
Change a card	In node view, right-click an OC-N card and choose **Change Card**. In the Change Card dialog box, choose the card type. Change card retains all card provisioning, including DCC terminations, protection, circuits, and ring. See also the "DLP-B247 Change an Optical Card" task on page 1-27.

Network View Tasks

Right-click the network view graphic area or a node, span, or domain to display shortcut menus. Table A-5 lists the actions that are available from the network view.

Table A-5 Network Management Tasks in Network View

Action	Task
Open a node	Any of the following: • Double-click a node icon. • Right-click a node icon and choose **Open Node** from the shortcut menu. • Click a node and choose **Go to Selected Object View** from the CTC View menu. • From the View menu, choose **Go To Other Node**. Select a node from the Select Node dialog box. • Double-click a node alarm or event in the Alarms or History tabs.
Move a node icon	Press the **Ctrl** key and the left mouse button simultaneously and drag the node icon to a new location.
Save a node icon position	On the network view map, right-click and choose **Save Node Position**. Click **Yes** on the **Save Node Position** dialog box.
Reset node icon position	Right-click a node and choose **Reset Node Position** from the shortcut menu. The node icon moves to the position defined by the longitude and latitude fields on the Provisioning > General tab in node view.

Table A-5 Network Management Tasks in Network View (continued)

Action	Task
Provision a circuit	Right-click a node. From the shortcut menu, choose **Provision Circuit To** and select the node where you want to provision the circuit. For circuit creation procedures, see Chapter 5, "Create Circuits and VT Tunnels."
Update circuits with new node	Right-click a node and choose **Update Circuits With New Node** from the shortcut menu. Use this command when you add a new node and want to pass circuits through it.
Display a link end point	Right-click a span. From the shortcut menu, choose **Go To [node/slot/port]** for the drop port you want to view. CTC displays the card in card view.
Display span properties	Any of the following: • Move your mouse over a span; the properties appear near the span. • Click a span; the properties appear in the upper left corner of the window. • Right-click a span; the properties appear at the top of the shortcut menu.
Perform a UPSR protection switch for an entire span	Right-click a network span and click **Circuits**. In the Circuits on Span dialog box, switch options are displayed in the UPSR Span Switching field. See also the "DLP-B197 Initiate a UPSR Force Switch" task on page 13-16.
Upgrade a span	Right-click a span and choose **Upgrade Span** from the shortcut menu. **Note** For detailed span upgrade information and instructions, see Chapter 11, "Upgrade Cards and Spans."

Table Display Options

Right-clicking a table column displays a menu. Table A-6 shows table display options, which include rearranging or hiding CTC table columns and sorting table columns by primary or secondary keys.

Table A-6 Table Display Options

Task	Click	Right-Click Shortcut Menu
Resize column	Left-click while dragging the header separator to the right or left.	—
Rearrange column order	Left-click while dragging the column header to the right or left.	—
Reset column order	—	Choose **Reset Columns Order/Visibility**.
Hide column	—	Choose **Hide Column**.
Show column	—	Choose **Show Column >** *column_name*
Display all hidden columns	—	Choose **Reset Columns Order/Visibility**.
Sort table (primary)	Click a column header; each click changes the sort order (ascending or descending).	Choose **Sort Column**.

Table A-6 Table Display Options (continued)

Task	Click	Right-Click Shortcut Menu
Sort table (secondary sorting keys)	Press the **Shift** key and simultaneously click the column header.	Choose **Sort Column (incremental)**.
Reset sorting	—	Choose **Reset Sorting**.
View table row count (Row Count is the last item on the shortcut menu) View the number listed next to "Row Count," it is the last item on the shortcut menu.	—	—

Equipment Inventory

In node view, the Inventory tab displays information about the ONS 15327 equipment, including:

- Delete Button—After highlighting a card with your mouse, use this button to delete the card from node view. See also the "DLP-B320 Delete a Card" task on page 1-26.
- Reset Button—After highlighting a card with your mouse, use this button to reset a card.
- Location—Where the equipment is installed, either chassis or slot number.
- Eqpt Type—Displays the type of equipment but not the specific card name, for example, OC12 or MIC.
- Actual Eqpt Type—Displays the actual equipment type, for example, 15327-OC48-1.
- HW Part #—Hardware part number; this number is printed on the top of the card or equipment piece.
- HW Rev—Hardware revision number.
- Serial #—Equipment 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 ONS 15327 cards.

APPENDIX B

Shelf Assembly Specifications

This appendix contains hardware and software specifications for the ONS 15327.

Bandwidth

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

Slot Assignments

- Total card slots: 8
- Traffic card slots (E10/100-4, G-1000-2, OC-3, OC-12, and OC-48): Slots 1 through 4
- XTC (Cross Connect, Timing and Control): Slots 5, 6
- MIC (Mechanical Interface Card): Slots 7, 8

Cards

- XTC-14
- XTC-28-3
- MIC A
- MIC B
- E10/100-4
- G1000-2
- OC-3 IR 4 1310
- OC-12 IR 1310
- OC-12 LR 1550
- OC-48 IR 1310
- OC-48 LR-1550

Warning **The OC-3, OC-12, OC-48, and E1000-2 cards are Class 1 laser products (IEC 60825-1 2001-01/Class I laser product (21CFR 1040.10 and 1040.11).**

Configurations

- Two-fiber UPSR
- Path protected mesh network (PPMN)
- Two-fiber BLSR
- Add-drop multiplexer
- Point-to-point terminal mode

Cisco Transport Controller

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

External LAN Interface

- 10 Base-T Ethernet

TL1 Craft Interface

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

Modem Interface

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

Alarm Interface

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

Nonvolatile Memory

- 96 MB, FLASH memory

BITS Interface

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

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

Power Specifications

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

Environmental Specifications

- Operating Temperature: 0 to +55 degrees Celsius; -40 to +65 degrees Celsius with industrial temperature rated cards
- Operating Humidity: 5 - 95%, non-condensing

Dimensions

- Height: 5.1 inches (13. cm)
- Width: 19 or 23 inches (41.8 or 50.6 cm) with mounting ears attached
- Depth: 11 inches (28 cm)
- Weight: 15 lb. empty (with fan tray assembly); (27 lb. maximum)

APPENDIX C

Network Element Defaults

This appendix describes the factory-configured (default) network element (NE) settings for the Cisco ONS 15327. It includes descriptions of card default settings and node default settings and provides procedures for importing, exporting and editing the settings. Ethernet card settings are not included in the factory-configured settings.

To change card settings individually (that is, without changing the defaults), see Chapter 9, "Change Port Settings." To change node settings without changing the defaults, see Chapter 10, "Change Node Settings."

Network Element Defaults Description

The NE defaults are pre-installed on each ONS 15327 XTC card. They also ship as a file called 15327-defaults.txt on the CTC software CD in the event you want to import the defaults onto existing XTC cards. The NE defaults include card-level and node-level defaults.

Changes made manually using Chapter 9, "Change Port Settings"override the default settings. If you use the Defaults Editor or import a new defaults file, that is, if defaults are changed, the changes apply only to cards installed or to slots pre-provisioned after the manual changes were made. A new defaults file will not take effect for cards already installed or ports slots already pre-provisioned when the change takes place.

Changes made manually to the node-level default settings (either when you initially turn up a node or change node settings later) override the default settings. If you change the default settings using the Defaults Editor or by importing a new defaults file, the new defaults take effect immediately for all settings except those relating to UPSR, BLSR, or 1+1 protection.

Use the following procedures if you need to edit, import, or export NE defaults.

NTP-B164 Edit Network Element Defaults

Purpose	This procedure edits the NE defaults using the NE Defaults Editor. The new defaults can either be applied only to the login node or exported to a file and imported for use on other nodes.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

Step 2 Click the **Provisioning > Defaults Editor** tabs.

Step 3 In the Defaults Selector area, choose a card (if you are editing card-level defaults) or **NODE** (if you are editing node-level defaults). Click the node name at the top of the Defaults Selector column to list all available NE defaults under Property Name.

Step 4 Locate a default you want to change under Property Name.

Step 5 Click the **Default Value** column for the default property you are changing and choose a value from the drop-down menu (available for some node-level settings only), or type the new value. You can modify multiple default values before applying the changes.

Note If you click **Reset** before you click **Apply**, all values will return to their original settings.

Step 6 Click **Apply**.

Note If the property is unavailable, click the **Property Name** column to activate the Apply button.

Step 7 Click **Yes** on the conformation dialog box. The dialog box appears if you are modifying node-level defaults; it notifies you that applying defaults for node level attributes overrides current provisioning.

Note Changes to node settings take effect when you click **Apply**. Changes to the IIOP Listener Port setting reboots the XTC. Changes made to card settings using the Defaults Editor do not change the settings for cards that are currently installed or slots that are pre-provisioned for cards. Card settings must be manually changed using procedures in Chapter 9, "Change Port Settings."

Stop. You have completed this procedure.

NTP-B165 Import Network Element Defaults

Purpose	This procedure imports the NE defaults using the NE Defaults Editor. The defaults can either be imported from the CTC software CD (factory defaults) or from a customized file exported and saved from a node.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

Step 2 Click the **Provisioning > Defaults Editor** tabs.

Step 3 Click **Import**.

Step 4 If the correct file name and location do not appear in the Import Defaults from File dialog box, click **Browse** and browse to the file you are importing.

Step 5 When the correct file name and location appear in the dialog box (the correct file name is 15327-defaults.txt if you are importing the factory defaults), click **OK**.

A pencil icon will appear next to any default value that will be changed as a result of importing the new defaults file.

Step 6 Click **Apply**.

Step 7 Click **Yes** on the confirmation dialog box. The dialog box appears if you are modifying node-level defaults; it notifies you that applying defaults for node level attributes overrides current provisioning.

Note Changes to node settings take effect when you click Apply. Changes to the IIOP Listener Port setting reboots the XTC. Changes made to card settings using the Defaults Editor do not change the settings for cards that are currently installed or slots that are pre-provisioned for cards. Card settings must be manually changed by using the procedures in Chapter 9, "Change Port Settings."

Stop. You have completed this procedure.

NTP-B166 Export Network Element Defaults

Purpose	This procedure exports the NE defaults using the NE Defaults Editor. The exported defaults can be imported to other nodes.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 Complete the "DLP-B60 Log into CTC" task on page 2-23. If you are already logged in, continue with Step 2.

Step 2 Click the **Provisioning > Defaults Editor** tabs.

Step 3 Click **Export**.

Step 4 If the file it does not appear in the Export Defaults to File dialog box, Click **Browse** and browse to the location where you want to export the file

Step 5 Change the file name to something easy to remember (the file name has no extension).

Step 6 Click **OK**.

Stop. You have completed this procedure.

Card Default Settings

The tables in this section list the default settings for each card. Cisco provides the following settings pre-provisioned for the ONS 15327 optical cards and electrical ports:

- Soak Time (all cards) is the length of time that elapses between an AINS port receiving a valid signal and when it automatically changes to in-service status.
- Line Coding (DS-1 ports) defines the DS-1 transmission coding type that is used.
- Line Length (DS-1 ports) defines the distance (in feet) from the backplane connection to the next termination point.
- Line Type (DS-1 ports) defines the type of framing used.
- Port State (all cards) sets the port to one of the four available states (IS, OOS, OOS_MT, or OOS_AINS), depending on whether you need ports in or out of service. Refer to the *Cisco ONS 15327 Reference Manual* for a complete description of the port states.
- SF BER Level (OC-N cards) defines the signal fail bit error rate.
- SD BER Level (OC-N cards) defines the signal degrade bit error rate.
- Enable Synch Messages (OC-N cards) enables synchronization status messages (S1 byte), which allow the node to choose the best timing source.
- STS IPPM Enabled (OC-N cards) enables intermediate-path performance monitoring on a node for transparent monitoring of a channel that does not terminate on that node.
- Send Do Not Use (OC-N cards) sends a DUS message on the S1 byte when enabled.

- PM Threshold Settings (all cards) set the performance monitoring parameters for gathering performance data and detecting problems early.

Table C-1 lists the DS-1 default settings.

Table C-1 DS-1 Default Settings

Property Name	Default Value
XTCDS1.config.AINSSoakTime	08:00 (hours:mins)
XTCDS1.config.LineCoding	AMI
XTCDS1.config.LineLength	0-131 (feet)
XTCDS1.config.LineType	D4
XTCDS1XTCDS1.config.State	OOS
XTCDS1.pmthresholds.line.farend.15min.ES	65 (seconds)
XTCDS1.pmthresholds.line.farend.1day.ES	648 (seconds)
XTCDS1.pmthresholds.line.nearend.15min.CV	13340 (BPV count)
XTCDS1.pmthresholds.line.nearend.15min.ES	65 (seconds)
XTCDS1.pmthresholds.line.nearend.15min.LOSS	10 (seconds)
XTCDS1.pmthresholds.line.nearend.15min.SES	10 (seconds)
XTCDS1.pmthresholds.line.nearend.1day.CV	133400 (BPV count)
XTCDS1.pmthresholds.line.nearend.1day.ES	648 (seconds)
XTCDS1.pmthresholds.line.nearend.1day.LOSS	10 (seconds)
XTCDS1.pmthresholds.line.nearend.1day.SES	100 (seconds)
XTCDS1.pmthresholds.path.farend.15min.CSS	25 (seconds)
XTCDS1.pmthresholds.path.farend.15min.CV	13296 (BIP count)
XTCDS1.pmthresholds.path.farend.15min.ES	65 (seconds)
XTCDS1.pmthresholds.path.farend.15min.ESA	25 (seconds)
XTCDS1.pmthresholds.path.farend.15min.ESB	25 (seconds)
XTCDS1.pmthresholds.path.farend.15min.SEFS	25 (seconds)
XTCDS1.pmthresholds.path.farend.15min.SES	10 (seconds)
XTCDS1.pmthresholds.path.farend.15min.UAS	10 (seconds)
XTCDS1.pmthresholds.path.farend.1day.CSS	25 (seconds)
XTCDS1.pmthresholds.path.farend.1day.CV	132960 (BIP count)
XTCDS1.pmthresholds.path.farend.1day.ES	648 (seconds)
XTCDS1.pmthresholds.path.farend.1day.ESA	25 (seconds)
XTCDS1.pmthresholds.path.farend.1day.ESB	25 (seconds)
XTCDS1.pmthresholds.path.farend.1day.SEFS	25 (seconds)
XTCDS1.pmthresholds.path.farend.1day.SES	100 (seconds)
XTCDS1.pmthresholds.path.farend.1day.UAS	10 (seconds)
XTCDS1.pmthresholds.path.nearend.15min.AISS	10 (seconds)
XTCDS1.pmthresholds.path.nearend.15min.CV	13296 (BIP count)

Table C-1 DS-1 Default Settings (continued)

Property Name	Default Value
XTCDS1.pmthresholds.path.nearend.15min.ES	65 (seconds)
XTCDS1.pmthresholds.path.nearend.15min.SAS	2 (seconds)XTCDS3
XTCDS1.pmthresholds.path.nearend.15min.SES	10 (seconds)
XTCDS1.pmthresholds.path.nearend.15min.UAS	10 (seconds)
XTCDS1.pmthresholds.path.nearend.1day.AISS	10 (seconds)
XTCDS1.pmthresholds.path.nearend.1day.CV	132960 (BIP count)
XTCDS1.pmthresholds.path.nearend.1day.ES	648 (seconds)
XTCDS1.pmthresholds.path.nearend.1day.SAS	17 (seconds)
XTCDS1.pmthresholds.path.nearend.1day.SES	100 (seconds)
XTCDS1.pmthresholds.path.nearend.1day.UAS	10 (seconds)
XTCDS1.pmthresholds.sts.farend.15min.CV	15 (B3 count)
XTCDS1.pmthresholds.sts.farend.15min.ES	12 (seconds)
XTCDS1.pmthresholds.sts.farend.15min.FC	10 (count)
XTCDS1.pmthresholds.sts.farend.15min.SES	3 (seconds)
XTCDS1.pmthresholds.sts.farend.15min.UAS	10 (seconds)
XTCDS1.pmthresholds.sts.farend.1day.CV	125 (B3 count)
XTCDS1.pmthresholds.sts.farend.1day.ES	100 (seconds)
XTCDS1.pmthresholds.sts.farend.1day.FC	10 (count)
XTCDS1.pmthresholds.sts.farend.1day.SES	7 (seconds)
XTCDS1.pmthresholds.sts.farend.1day.UAS	10 (seconds)
XTCDS1.pmthresholds.sts.nearend.15min.CV	15 (B3 count)
XTCDS1.pmthresholds.sts.nearend.15min.ES	12 (seconds)
XTCDS1.pmthresholds.sts.nearend.15min.FC	10 (count)
XTCDS1.pmthresholds.sts.nearend.15min.SES	3 (seconds)
XTCDS1.pmthresholds.sts.nearend.15min.UAS	10 (seconds)
XTCDS1.pmthresholds.sts.nearend.1day.CV	125 (B3 count)
XTCDS1.pmthresholds.sts.nearend.1day.ES	100 (seconds)
XTCDS1.pmthresholds.sts.nearend.1day.FC	10 (count)
XTCDS1.pmthresholds.sts.nearend.1day.SES	7 (seconds)
XTCDS1.pmthresholds.sts.nearend.1day.UAS	10 (seconds)
XTCDS1.pmthresholds.vt.farend.15min.CV	15 (BIP8 count)
XTCDS1.pmthresholds.vt.farend.15min.ES	12 (seconds)
XTCDS1.pmthresholds.vt.farend.15min.SES	3 (seconds)
XTCDS1.pmthresholds.vt.farend.15min.UAS	10 (seconds)
XTCDS1.pmthresholds.vt.farend.1day.CV	125 (BIP8 count)
XTCDS1.pmthresholds.vt.farend.1day.ES	100 (seconds)

Table C-1 DS-1 Default Settings (continued)

Property Name	Default Value
XTCDS1.pmthresholds.vt.farend.1day.SES	7 (seconds)
XTCDS1.pmthresholds.vt.farend.1day.UAS	10 (seconds)
XTCDS1.pmthresholds.vt.nearend.15min.CV	15 (BIP8 count)
XTCDS1.pmthresholds.vt.nearend.15min.ES	12 (seconds)
XTCDS1.pmthresholds.vt.nearend.15min.SES	3 (seconds)
XTCDS1.pmthresholds.vt.nearend.15min.UAS	10 (seconds)
XTCDS1.pmthresholds.vt.nearend.1day.CV	125 (BIP8 count)
XTCDS1.pmthresholds.vt.nearend.1day.ES	100 (seconds)
XTCDS1.pmthresholds.vt.nearend.1day.SES	7 (seconds)
XTCDS1.pmthresholds.vt.nearend.1day.UAS	10 (seconds)

Table C-2 lists the DS-3 default settings.

Table C-2 DS-3 Default Settings

Property Name	Default Value
XTCDS3.config.AINSSoakTime	08:00 (hours:mins)
XTCDS3.config.LineLength	0-225 (feet)
XTCDS3.config.State	OOS
XTCDS3.pmthresholds.line.nearend.15min.CV	387 (BPV count)
XTCDS3.pmthresholds.line.nearend.15min.ES	25 (seconds)
XTCDS3.pmthresholds.line.nearend.15min.LOSS	10 (seconds)
XTCDS3.pmthresholds.line.nearend.15min.SES	4 (seconds)
XTCDS3.pmthresholds.line.nearend.1day.CV	3865 (BPV count)
XTCDS3.pmthresholds.line.nearend.1day.ES	250 (seconds)
XTCDS3.pmthresholds.line.nearend.1day.LOSS	10 (seconds)
XTCDS3.pmthresholds.line.nearend.1day.SES	40 (seconds)
XTCDS3.pmthresholds.sts.farend.15min.CV	15 (G1 count)
XTCDS3.pmthresholds.sts.farend.15min.ES	12 (seconds)
XTCDS3.pmthresholds.sts.farend.15min.FC	10 (count)
XTCDS3.pmthresholds.sts.farend.15min.SES	3 (seconds)
XTCDS3.pmthresholds.sts.farend.15min.UAS	10 (seconds)
XTCDS3.pmthresholds.sts.farend.1day.CV	125 (G1 count)
XTCDS3.pmthresholds.sts.farend.1day.ES	100 (seconds)
XTCDS3.pmthresholds.sts.farend.1day.FC	10 (count)
XTCDS3.pmthresholds.sts.farend.1day.SES	7 (seconds)
XTCDS3.pmthresholds.sts.farend.1day.UAS	10 (seconds)

Table C-2 DS-3 Default Settings (continued)

Property Name	Default Value
XTCDS3.pmthresholds.sts.nearend.15min.CV	15 (B3 count)
XTCDS3.pmthresholds.sts.nearend.15min.ES	12 (seconds)
XTCDS3.pmthresholds.sts.nearend.15min.FC	10 (count)
XTCDS3.pmthresholds.sts.nearend.15min.SES	3 (seconds)
XTCDS3.pmthresholds.sts.nearend.15min.UAS	10 (seconds)
XTCDS3.pmthresholds.sts.nearend.1day.CV	125 (B3 count)
XTCDS3.pmthresholds.sts.nearend.1day.ES	100 (seconds)
XTCDS3.pmthresholds.sts.nearend.1day.FC	10 (count)
XTCDS3.pmthresholds.sts.nearend.1day.SES	7 (seconds)
XTCDS3.pmthresholds.sts.nearend.1day.UAS	10 (seconds)

Table C-3 lists the default settings for the OC-3 card.

Table C-3 OC-3 Card Default Settings

Property Name	Default Value
OC3.config.line.AINSSoakTime	08:00 (hours:mins)
OC3.config.line.EnableSyncMsg	TRUE
OC3.config.line.PJStsMon#	0 (STS #)
OC3.config.line.SDBER	1E-7
OC3.config.line.SFBER	1E-4
OC3.config.line.SendDoNotUse	FALSE
OC3.config.line.State	OOS
OC3.config.sts.IPPMEnabled	FALSE
OC3.pmthresholds.line.farend.15min.CV	1312 (B2 count)
OC3.pmthresholds.line.farend.15min.ES	87 (seconds)
OC3.pmthresholds.line.farend.15min.FC	10 (count)
OC3.pmthresholds.line.farend.15min.SES	1 (seconds)
OC3.pmthresholds.line.farend.15min.UAS	3 (seconds)
OC3.pmthresholds.line.farend.1day.CV	13120 (B2 count)
OC3.pmthresholds.line.farend.1day.ES	864 (seconds)
OC3.pmthresholds.line.farend.1day.FC	40 (count)
OC3.pmthresholds.line.farend.1day.SES	4 (seconds)
OC3.pmthresholds.line.farend.1day.UAS	10 (seconds)
OC3.pmthresholds.line.nearend.15min.CV	1312 (B2 count)
OC3.pmthresholds.line.nearend.15min.ES	87 (seconds)
OC3.pmthresholds.line.nearend.15min.FC	10 (count)

Table C-3 OC-3 Card Default Settings (continued)

Property Name	Default Value
OC3.pmthresholds.line.nearend.15min.NPJC-PDET	60 (count)
OC3.pmthresholds.line.nearend.15min.NPJC-PGEN	60 (count)
OC3.pmthresholds.line.nearend.15min.PPJC-PDET	60 (count)
OC3.pmthresholds.line.nearend.15min.PPJC-PGEN	60 (count)
OC3.pmthresholds.line.nearend.15min.PSC	1 (count)
OC3.pmthresholds.line.nearend.15min.PSD	300 (seconds)
OC3.pmthresholds.line.nearend.15min.SES	1 (seconds)
OC3.pmthresholds.line.nearend.15min.UAS	3 (seconds)
OC3.pmthresholds.line.nearend.1day.CV	13120 (B2 count)
OC3.pmthresholds.line.nearend.1day.ES	864 (seconds)
OC3.pmthresholds.line.nearend.1day.FC	40 (count)
OC3.pmthresholds.line.nearend.1day.NPJC-PDET	5760 (count)
OC3.pmthresholds.line.nearend.1day.NPJC-PGEN	5760 (count)
OC3.pmthresholds.line.nearend.1day.PPJC-PDET	5760 (count)
OC3.pmthresholds.line.nearend.1day.PPJC-PGEN	5760 (count)
OC3.pmthresholds.line.nearend.1day.PSC	5 (count)
OC3.pmthresholds.line.nearend.1day.PSD	600 (seconds)
OC3.pmthresholds.line.nearend.1day.SES	4 (seconds)
OC3.pmthresholds.line.nearend.1day.UAS	10 (seconds)
OC3.pmthresholds.section.nearend.15min.CV	1000 (B1 count)
OC3.pmthresholds.section.nearend.15min.ES	500 (seconds)
OC3.pmthresholds.section.nearend.15min.SEFS	500 (seconds)
OC3.pmthresholds.section.nearend.15min.SES	500 (seconds)
OC3.pmthresholds.section.nearend.1day.CV	100000 (B1 count)
OC3.pmthresholds.section.nearend.1day.ES	5000 (seconds)
OC3.pmthresholds.section.nearend.1day.SEFS	5000 (seconds)
OC3.pmthresholds.section.nearend.1day.SES	5000 (seconds)
OC3.pmthresholds.sts.nearend.15min.CV	15 (B3 count)
OC3.pmthresholds.sts.nearend.15min.ES	12 (seconds)
OC3.pmthresholds.sts.nearend.15min.FC	10 (count)
OC3.pmthresholds.sts.nearend.15min.SES	3 (seconds)
OC3.pmthresholds.sts.nearend.15min.UAS	10 (seconds)
OC3.pmthresholds.sts.nearend.1day.CV	125 (B3 count)
OC3.pmthresholds.sts.nearend.1day.ES	100 (seconds)
OC3.pmthresholds.sts.nearend.1day.FC	10 (count)

Table C-3 OC-3 Card Default Settings (continued)

Property Name	Default Value
OC3.pmthresholds.sts.nearend.1day.SES	7 (seconds)
OC3.pmthresholds.sts.nearend.1day.UAS	10 (seconds)

Table C-4 lists the default settings for the OC-12 card.

Table C-4 OC-12 Card Default Settings

Property Name	Default Value
OC12.config.line.AINSSoakTime	08:00 (hours:mins)
OC12.config.line.EnableSyncMsg	TRUE
OC12.config.line.PJStsMon#	0 (STS #)
OC12.config.line.SDBER	1E-7
OC12.config.line.SFBER	1E-4
OC12.config.line.SendDoNotUse	FALSE
OC12.config.line.State	OOS
OC12.config.sts.IPPMEnabled	FALSE
OC12.pmthresholds.line.farend.15min.CV	5315 (B2 count)
OC12.pmthresholds.line.farend.15min.ES	87 (seconds)
OC12.pmthresholds.line.farend.15min.FC	10 (count)
OC12.pmthresholds.line.farend.15min.SES	1 (seconds)
OC12.pmthresholds.line.farend.15min.UAS	3 (seconds)
OC12.pmthresholds.line.farend.1day.CV	53150 (B2 count)
OC12.pmthresholds.line.farend.1day.ES	864 (seconds)
OC12.pmthresholds.line.farend.1day.FC	40 (count)
OC12.pmthresholds.line.farend.1day.SES	4 (seconds)
OC12.pmthresholds.line.farend.1day.UAS	10 (seconds)
OC12.pmthresholds.line.nearend.15min.CV	5315 (B2 count)
OC12.pmthresholds.line.nearend.15min.ES	87 (seconds)
OC12.pmthresholds.line.nearend.15min.FC	10 (count)
OC12.pmthresholds.line.nearend.15min.NPJC-PDET	60 (count)
OC12.pmthresholds.line.nearend.15min.NPJC-PGEN	60 (count)
OC12.pmthresholds.line.nearend.15min.PPJC-PDET	60 (count)
OC12.pmthresholds.line.nearend.15min.PPJC-PGEN	60 (count)
OC12.pmthresholds.line.nearend.15min.PSC	1 (count)
OC12.pmthresholds.line.nearend.15min.PSC-W	1 (count)
OC12.pmthresholds.line.nearend.15min.PSD	300 (seconds)
OC12.pmthresholds.line.nearend.15min.PSD-W	300 (seconds)

Table C-4 OC-12 Card Default Settings (continued)

Property Name	Default Value
OC12.pmthresholds.line.nearend.15min.SES	1 (seconds)
OC12.pmthresholds.line.nearend.15min.UAS	3 (seconds)
OC12.pmthresholds.line.nearend.1day.CV	53150 (B2 count)
OC12.pmthresholds.line.nearend.1day.ES	864 (seconds)
OC12.pmthresholds.line.nearend.1day.FC	40 (count)
OC12.pmthresholds.line.nearend.1day.NPJC-PDET	5760 (count)
OC12.pmthresholds.line.nearend.1day.NPJC-PGEN	5760 (count)
OC12.pmthresholds.line.nearend.1day.PPJC-PDET	5760 (count)
OC12.pmthresholds.line.nearend.1day.PPJC-PGEN	5760 (count)
OC12.pmthresholds.line.nearend.1day.PSC	5 (count)
OC12.pmthresholds.line.nearend.1day.PSC-W	5 (count)
OC12.pmthresholds.line.nearend.1day.PSD	600 (seconds)
OC12.pmthresholds.line.nearend.1day.PSD-W	600 (seconds)
OC12.pmthresholds.line.nearend.1day.SES	4 (seconds)
OC12.pmthresholds.line.nearend.1day.UAS	10 (seconds)
OC12.pmthresholds.section.nearend.15min.CV	1000 (B1 count)
OC12.pmthresholds.section.nearend.15min.ES	500 (seconds)
OC12.pmthresholds.section.nearend.15min.SEFS	500 (seconds)
OC12.pmthresholds.section.nearend.15min.SES	500 (seconds)
OC12.pmthresholds.section.nearend.1day.CV	100000 (B1 count)
OC12.pmthresholds.section.nearend.1day.ES	5000 (seconds)
OC12.pmthresholds.section.nearend.1day.SEFS	5000 (seconds)
OC12.pmthresholds.section.nearend.1day.SES	5000 (seconds)
OC12.pmthresholds.sts.nearend.15min.CV	15 (B3 count)
OC12.pmthresholds.sts.nearend.15min.ES	12 (seconds)
OC12.pmthresholds.sts.nearend.15min.FC	10 (count)
OC12.pmthresholds.sts.nearend.15min.SES	3 (seconds)
OC12.pmthresholds.sts.nearend.15min.UAS	10 (seconds)
OC12.pmthresholds.sts.nearend.1day.CV	125 (B3 count)
OC12.pmthresholds.sts.nearend.1day.ES	100 (seconds)
OC12.pmthresholds.sts.nearend.1day.FC	10 (count)
OC12.pmthresholds.sts.nearend.1day.SES	7 (seconds)
OC12.pmthresholds.sts.nearend.1day.UAS	10 (seconds)

Table C-5 lists the default settings for the OC-48 cards.

Table C-5 OC-48 Cards Default Settings

Property Name	Default Value
OC48.config.line.AINSSoakTime	08:00 (hours:mins)
OC48.config.line.EnableSyncMsg	TRUE
OC48.config.line.PJStsMon#	0 (STS #)
OC48.config.line.SDBER	1E-7
OC48.config.line.SFBER	1E-4
OC48.config.line.SendDoNotUse	FALSE
OC48.config.line.State	OOS
OC48.config.sts.IPPMEnabled	FALSE
OC48.pmthresholds.line.farend.15min.CV	21260 (B2 count)
OC48.pmthresholds.line.farend.15min.ES	87 (seconds)
OC48.pmthresholds.line.farend.15min.FC	10 (count)
OC48.pmthresholds.line.farend.15min.SES	1 (seconds)
OC48.pmthresholds.line.farend.15min.UAS	3 (seconds)
OC48.pmthresholds.line.farend.1day.CV	212600 (B2 count)
OC48.pmthresholds.line.farend.1day.ES	864 (seconds)
OC48.pmthresholds.line.farend.1day.FC	40 (count)
OC48.pmthresholds.line.farend.1day.SES	4 (seconds)
OC48.pmthresholds.line.farend.1day.UAS	10 (seconds)
OC48.pmthresholds.line.nearend.15min.CV	21260 (B2 count)
OC48.pmthresholds.line.nearend.15min.ES	87 (seconds)
OC48.pmthresholds.line.nearend.15min.FC	10 (count)
OC48.pmthresholds.line.nearend.15min.NPJC-PDET	60 (count)
OC48.pmthresholds.line.nearend.15min.NPJC-PGEN	60 (count)
OC48.pmthresholds.line.nearend.15min.PPJC-PDET	60 (count)
OC48.pmthresholds.line.nearend.15min.PPJC-PGEN	60 (count)
OC48.pmthresholds.line.nearend.15min.PSC	1 (count)
OC48.pmthresholds.line.nearend.15min.PSC-R	1 (count)
OC48.pmthresholds.line.nearend.15min.PSC-S	1 (count)
OC48.pmthresholds.line.nearend.15min.PSC-W	1 (count)
OC48.pmthresholds.line.nearend.15min.PSD	300 (seconds)
OC48.pmthresholds.line.nearend.15min.PSD-R	300 (seconds)
OC48.pmthresholds.line.nearend.15min.PSD-S	300 (seconds)
OC48.pmthresholds.line.nearend.15min.PSD-W	300 (seconds)
OC48.pmthresholds.line.nearend.15min.SES	1 (seconds)
OC48.pmthresholds.line.nearend.15min.UAS	3 (seconds)

Table C-5 OC-48 Cards Default Settings (continued)

Property Name	Default Value
OC48.pmthresholds.line.nearend.1day.CV	212600 (B2 count)
OC48.pmthresholds.line.nearend.1day.ES	864 (seconds)
OC48.pmthresholds.line.nearend.1day.FC	40 (count)
OC48.pmthresholds.line.nearend.1day.NPJC-PDET	5760 (count)
OC48.pmthresholds.line.nearend.1day.NPJC-PGEN	5760 (count)
OC48.pmthresholds.line.nearend.1day.PPJC-PDET	5760 (count)
OC48.pmthresholds.line.nearend.1day.PPJC-PGEN	5760 (count)
OC48.pmthresholds.line.nearend.1day.PSC	5 (count)
OC48.pmthresholds.line.nearend.1day.PSC-R	5 (count)
OC48.pmthresholds.line.nearend.1day.PSC-S	5 (count)
OC48.pmthresholds.line.nearend.1day.PSC-W	5 (count)
OC48.pmthresholds.line.nearend.1day.PSD	600 (seconds)
OC48.pmthresholds.line.nearend.1day.PSD-R	600 (seconds)
OC48.pmthresholds.line.nearend.1day.PSD-S	600 (seconds)
OC48.pmthresholds.line.nearend.1day.PSD-W	600 (seconds)
OC48.pmthresholds.line.nearend.1day.SES	4 (seconds)
OC48.pmthresholds.line.nearend.1day.UAS	10 (seconds)
OC48.pmthresholds.section.nearend.15min.CV	10000 (B1 count)
OC48.pmthresholds.section.nearend.15min.ES	500 (seconds)
OC48.pmthresholds.section.nearend.15min.SEFS	500 (seconds)
OC48.pmthresholds.section.nearend.15min.SES	500 (seconds)
OC48.pmthresholds.section.nearend.1day.CV	100000 (B1 count)
OC48.pmthresholds.section.nearend.1day.ES	5000 (seconds)
OC48.pmthresholds.section.nearend.1day.SEFS	5000 (seconds)
OC48.pmthresholds.section.nearend.1day.SES	5000 (seconds)
OC48.pmthresholds.sts.nearend.15min.CV	15 (B3 count)
OC48.pmthresholds.sts.nearend.15min.ES	12 (seconds)
OC48.pmthresholds.sts.nearend.15min.FC	10 (count)
OC48.pmthresholds.sts.nearend.15min.SES	3 (seconds)
OC48.pmthresholds.sts.nearend.15min.UAS	10 (seconds)
OC48.pmthresholds.sts.nearend.1day.CV	125 (B3 count)
OC48.pmthresholds.sts.nearend.1day.ES	100 (seconds)
OC48.pmthresholds.sts.nearend.1day.FC	10 (count)
OC48.pmthresholds.sts.nearend.1day.SES	7 (seconds)
OC48.pmthresholds.sts.nearend.1day.UAS	10 (seconds)

Node Default Settings

The table in this section lists the node-level default settings for the Cisco ONS 15327. Cisco provides the following types of settings pre-provisioned for each ONS 15327 node:

- UPSR reversion settings determine whether or not UPSR circuits are revertive and, if so, what the reversion time is.
- Defaults Description lists the current defaults file on the node.
- BLSR reversion settings determine whether or not BLSR circuits are revertive and, if so, what the reversion time is.
- IIOP Listener Port sets the IIOP listener port number.
- Login Warning Message warns users at the login screen about the possible legal or contractual ramifications of accessing equipment, systems, or networks without authorization.
- 1+1 protection settings determine whether or not 1+1 protected circuits are revertive and, if so, what the reversion time is.
- Timing settings determine the AIS threshold, coding, and framing for BITS1 and BITS2 timing.

Table C-6 lists the ONS 15327 node default settings.

Table C-6 Node Default Settings

Property Name	Default Value
NODE.circuits.CreateLikeTL1	FALSE
NODE.circuits.upsr.SDBER	1E-6
NODE.circuits.upsr.SFBER	1E-4
NODE.circuits.upsr.SwitchOnPDIP	FALSE
NODE.circuits.upsr.ReversionTime	5.0 (minutes)
NODE.circuits.upsr.Revertive	FALSE
NODE.general.CraftAccessOnly	FALSE
NODE.general.CtcIpDisplaySuppression	FALSE
NODE.general.DefaultsDescription	Factory Defaults
NODE.general.EnableFirewall	FALSE
NODE.general.EnableProxy	FALSE
NODE.general.IIOPListenerPort (reboots node)	57790 (port #)
NODE.general.LoginWarningMessage	LoginWarningMessage=<center><B>WARNING</B><center>This system is restricted to authorized users for business purposes. Unauthorized<p>access is a violation of the law. This service may be monitored for administrative<p> and security reasons. By proceeding, you consent to this monitoring.
NODE.general.NtpSntpServer	0.0.0.0
NODE.general.TimeZone	(GMT-08\:00) Los Angeles, Tijuana, Vancouver (Pacific)

Table C-6 Node Default Settings (continued)

Property Name	Default Value
NODE.general.UseDST	TRUE
NODE.general.UseNtpSntpServer	FALSE
NODE.protection.1+1.BidirectionalSwitching	FALSE
NODE.protection.1+1.ReversionTime	5.0 (minutes)
NODE.protection.1+1.Revertive	FALSE
NODE.protection.blsr.RingReversionTime	5.0 (minutes)
NODE.protection.blsr.RingRevertive	TRUE
NODE.protection.blsr.SpanReversionTime	5.0 (minutes)
NODE.protection.blsr.SpanRevertive	TRUE
NODE.security.policy.FailedLoginsBeforeLockout	5
NODE.security.policy.IdleUserTimeoutPolicy.Maintenance	60
NODE.security.policy.IdleUserTimeoutPolicy.Provisioning	30
NODE.security.policy.IdleUserTimeoutPolicy.Retrieve	0
NODE.security.policy.IdleUserTimeoutPolicy.Superuser	15
NODE.security.policy.LockoutDuration	00\:30
NODE.security.policy.ManualUnlockBySuperuser	FALSE
NODE.security.policy.PasswordReuseThreshold	1
NODE.security.policy.PasswordReuseTimeou	20
NODE.security.policy.SingleSessionPerUser	FALSE
NODE.timing.bits-1.AISThreshold	SMC
NODE.timing.bits-1.Coding	B8ZS
NODE.timing.bits-1.Framing	ESF
NODE.timing.bits-1.State	IS
NODE.timing.bits-2.AISThreshold	SMC
NODE.timing.bits-2.Coding	B8ZS
NODE.timing.bits-2.Framing	ESF
NODE.timing.bits-2.State	IS
NODE.timing.general.Mode	External
NODE.timing.general.QualityOfRES	RES=DUS
NODE.timing.general.ReversionTime	5.0 (minutes)
NODE.timing.general.Revertive	FALSE
NODE.timing.general.SSMMessageSet	Generation 1

Alternate Installation Procedures

This appendix describes installation procedures that can be used in place of some of the procedures contained in Chapter 1, "Install Hardware."

Before You Begin

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-B223 Install the Fiber-Optic Cable Storage Drawer, page D-2—As needed, complete this procedure to install the cable storage drawer that you can use to store slack cable.
2. NTP-B224 Route Cables Through the Fiber-Optic Cable Storage Drawer, page D-2—As needed, complete this procedure to route fiber-optic cable through the cable storage drawer.
3. NTP-B222 Connect Office Power to the ONS 15327 Shelf (Terminal-Lug Power Connector), page D-4—As needed, complete this procedure to connect office power using terminal-lug power connectors, rather than screw-type connectors.

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

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

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

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

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

NTP-B223 Install the Fiber-Optic Cable Storage Drawer

Purpose	This procedure installs the fiber-optic cable storage drawer used to store up to 5 feet of slack optical cable from the ONS 15327.
Tools/Equipment	Fiber-optic cable storage drawer Screws, 12-24 or 10-32 (4)
Prerequisite Procedures	DLP-B5 Mount the ONS 15327 in a Rack, page 1-8
Required/As Needed	As needed to store extra fiber cable
Onsite/Remote	Onsite
Security Level	None

Note A single cable storage drawer can hold slack cable from up to two ONS 15327s.

Step 1 Align the mounting holes on the bracket with the mounting holes in the equipment rack located 2 RUs below the lowest piece of installed equipment (ONS 15327 or tie-down bar).

Note If you are using a tie-down bar to manage cables, you must install the cable storage drawer under the bar.

Step 2 Install the four 12-24 or 10-32 screws through the elongated holes in the brackets and into the threaded holes in the mounting posts.

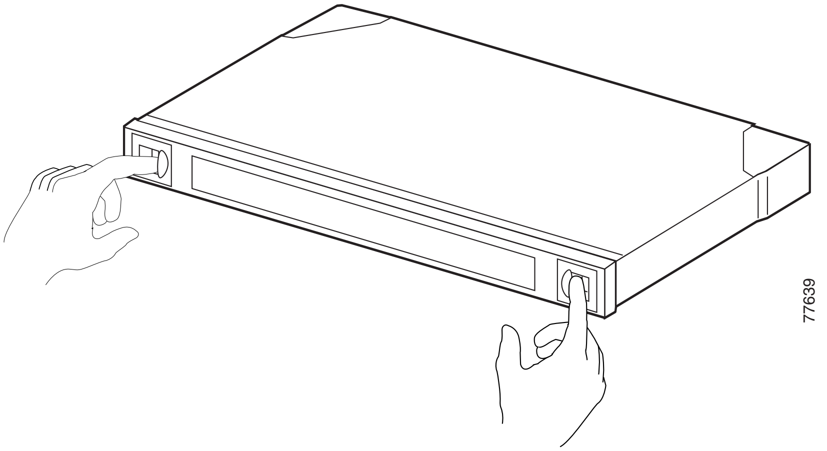
Step 3 **Stop. You have completed this procedure.**

NTP-B224 Route Cables Through the Fiber-Optic Cable Storage Drawer

Purpose	This procedure routes excess cable through the cable storage drawer.
Tools/Equipment	None
Prerequisite Procedures	NTP-B223 Install the Fiber-Optic Cable Storage Drawer, page D-2
Required/As Needed	As needed to route and store extra fiber cable
Onsite/Remote	Onsite
Security Level	None

Step 1 Open the cable storage drawer by pushing in the tabs to release the locked drawer (Figure D-1).

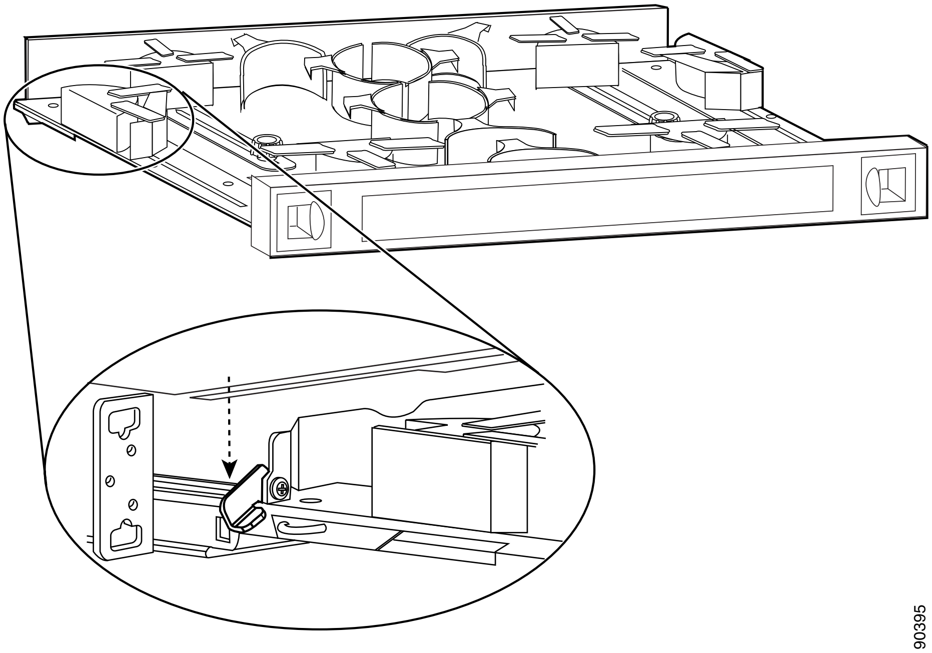
Figure D-1 Opening the Fiber-Optic Cable Storage Drawer



Step 2 Pull out the cable storage drawer.

Step 3 Lock the drawer in the open position by pushing the latch at drawer down into the lock position (Figure D-2).

Figure D-2 Locking the Cable Storage Drawer



Step 4 Route the cable down the left side of the chassis and into the drawer.

Step 5 Continue to route the cable through the drawer around the round cable retainers to the right side.

Step 6 Pull the cable up out of the right side of the drawer

Step 7 Repeat Steps 4 through 6 to continue cabling the system.

Step 8 Unlock the drawer by moving the latch back into an upright position and close the drawer.

Step 9 Push the drawer shut until it clicks in place.

Step 10 **Stop. You have completed this procedure.**

NTP-B222 Connect Office Power to the ONS 15327 Shelf (Terminal-Lug Power Connector)

Purpose	This procedure connects power to the ONS 15327 shelf.
Tools/Equipment	#2 Phillips screwdriver Medium slot head screwdriver Small slot head screwdriver Wire wrapper Wire cutters Wire strippers Crimp tool Fuse panel Terminal-lug power connectors (2) Terminal lugs (4) Terminal lug screws (4) Power cable (from fuse and alarm panel to assembly), #10 AWG, copper conductors, 194°F [90°C]) Ground cable #6 AWG stranded Listed pressure terminal connectors such as ring and fork types; connectors must be suitable for #10 AWG copper conductors Labels (2) (one for the A-side power lead and one for the B-side)
Prerequisite Procedures	DLP-B16 Connect the Office Ground to the ONS 15327, page 1-13
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Note This procedure describes the installation of the terminal-lug power connector. To install the screw-lock power connector also included with the ONS 15327, see the "DLP-B17 Connect Office Power to the ONS 15327 Shelf (Screw-Lock Power Connector)" task on page 1-14.

Note If you encounter problems with the power supply, refer to the *Cisco ONS 15327 Troubleshooting Guide*.

Warning **Do not apply power to the ONS 15327 until you complete all installation steps and check the continuity of the -48 VDC and return.**

Step 1 Connect the office power according to the fuse panel engineering specifications.

Step 2 Measure and cut the cables as needed to reach the ONS 15327 from the fuse panel.

Step 3 Dress the power according to local site practice.

Warning **When installing the ONS 15327, the ground connection must always be made first and disconnected last.**

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

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

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

Note To install the terminal-lug power connector, see the "NTP-B222 Connect Office Power to the ONS 15327 Shelf (Terminal-Lug Power Connector)" procedure on page D-4.

Step 5 If the power connector is already installed, remove it from the MIC by grasping it with your fingers and gently pulling it. If you cannot remove it easily, you can use a pair of needle nose pliers and grab it by the center of the channel.

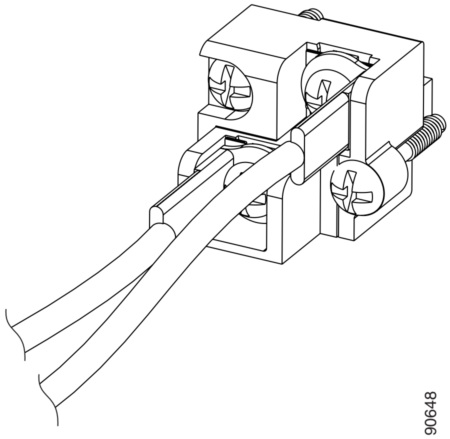
Step 6 Crimp the terminal lugs to the power cables.

Step 7 Remove the terminal lug screws and discard.

Step 8 Insert the return (black) power cable in the right hand (RET) slot of the connector. Figure D-3 show the proper orientation of the terminal lugs.

Warning **Make sure the flat part of the lug faces away from the center of the connector.**

Figure D-3 MIC Terminal-Lug Power Connector



Step 9 Secure the lug using the screws provided.

Step 10 Insert the battery (red) wire into the left hand (–48V) slot of the connector.

Warning **Make sure the flat part of the lug faces away from the center of the connector.**

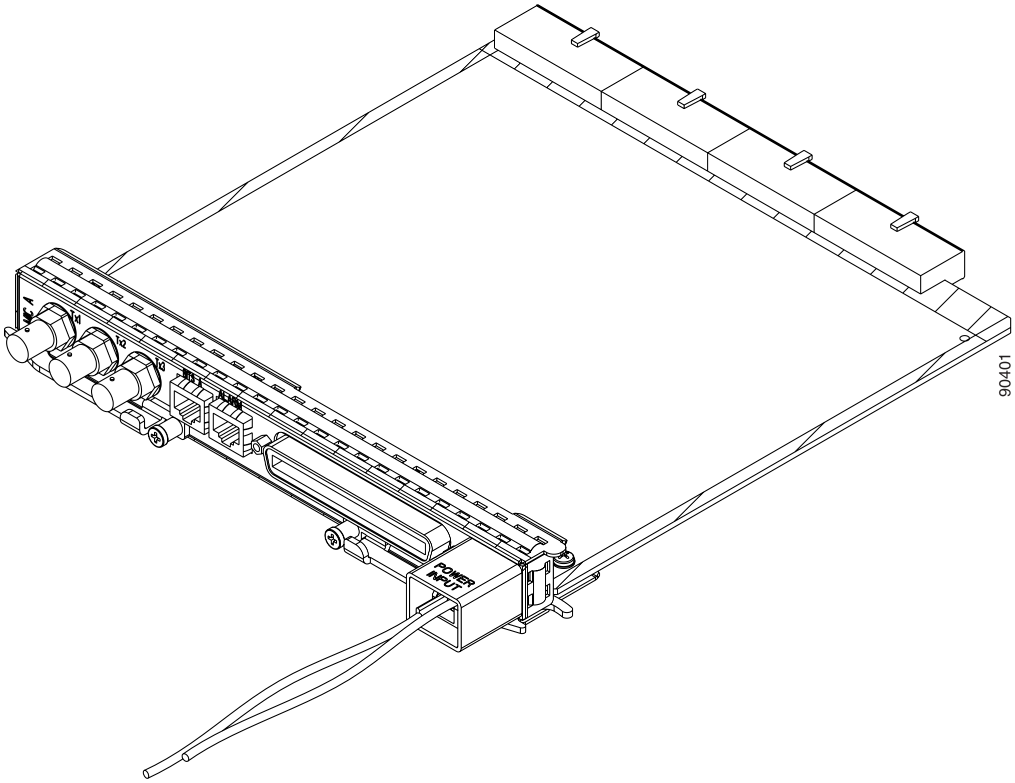
Step 11 Secure the battery (–48V) wire using the screws provided.

Step 12 Place the plastic shroud over the power connector and plug the power connector into the MIC.

Step 13 Secure the connector to the shelf using the top left and bottom right screws.

Figure D-4 shows power cables connected to the terminal-lug power connector on the MIC.

Figure D-4 Power Cable Inserted into the MIC Terminal-Lug Power Connector



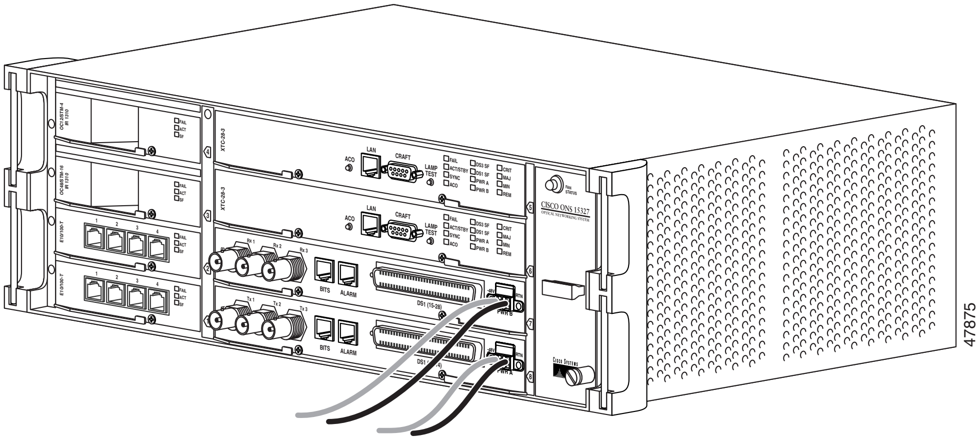
Step 14 If you use redundant power leads, repeat Steps 5 through 12 for the other MIC.

Step 15 Use the "PWR A" and "PWR B" labels provided with the MIC to designate the power leads.

Caution In case a power cable is damaged or cut, Cisco recommends that you diversely route redundant power leads along different paths. If you installed the tie-down bar, you can run one power lead across the tie-down bar and secure it using tie-wraps or other site-specific methods. You should route the other power cable in the opposite direction.

Figure D-5 shows redundant power connected to an ONS 15327.

Figure D-5 Redundant Power Connected to an ONS 15327



Stop. You have completed this procedure.

GLOSSARY

Numerics

1:1 protection

An electrical card protection scheme that pairs a working card with a protect card of the same type in an adjacent slot (DS-1 and DS-3 speeds). If the working card fails, the traffic from the working card switches to the protect card. When the failure on the working card is resolved, traffic reverts to the working card.

1+1 protection

An optical (OC-N) card protection scheme that pairs a single working port/card with a single dedicated protect port/card. All OC-N cards can use this protection type (OC-3, OC-12, OC-48, and OC-192 speeds).

1:N protection

An electrical card protection scheme that allows a single protect card to provide protection for several working cards (DS-1 and DS-3 speeds). If a working card fails, the traffic from the working card switches to the protect card.When the failure on the working card is resolved, traffic reverts to the working card.

10BaseT

Standard 10 Mbps local area network over unshielded twisted pair copper wire.

100BaseT

Standard 100 Mbps local ethernet network.

100BaseTX

Specification of 100BaseT that supports full duplex operation.

A

Access drop

Points where network devices can access the network.

ACO

Alarm cutoff.

Active card

A card that is working or carrying traffic. A card provisioned as working can be an active card or, after a protection switch, a protect card can be an active card.

ACT/STBY

Active/Standby.

Address mask

Bit combination used to describe the portion of an IP address that refers to the network or subnet and the portion that refers to the host. Sometimes referred to as mask. See also *subnet mask*.

ADM

(Add/drop multiplexers). Linear ADMs allow signals to be added to a SONET span or dropped from a SONET span. An ADM has three or more nodes.

Agent

1. 1. Generally, software that processes queries and returns replies on behalf of an application.
2. 2. In a network management system, a process that resides in all managed devices and reports the values of specified variables to management stations.

AIC

Alarm Interface Controller.

AID

(Access Identifier). An access code used in TL1 messaging that identifies and addresses specific objects within the ONS 15454. These objects include individual pieces of equipment, transport spans, access tributaries, and others. See also *TID*.

AIP

Alarm Interface Panel.

AIS

Alarm Indication Signal.

AIS-L

Line Alarm Indication Signal.

AMI

(Alternate Mark Inversion). Line-code format used on T1 circuits that transmits ones by alternate positive and negative pulses. Zeroes are represented by 01 during each bit cell and ones are represented by 11 or 00, alternately, during each bit cell. AMI requires that the sending device maintain ones density. Ones density is not maintained independently of the data stream. Sometimes called binary-coded alternate mark inversion.

ANSI

American National Standards Institute.

APS

(Automatic Protection Switching). SONET switching mechanism that routes traffic from working lines to protect lines if a line card failure or fiber cut occurs.

ARP

Address Resolution Protocol.

APSB

Alarm Protection Switching Byte.

ATAG

(Autonomous Message Tag). ATAG is used for TL1 message sequencing. See also *CTAG*.

ATM

Asynchronous Transfer Mode.

AWG

American Wire Gauge

B

B8ZS

(Binary 8-zero Substitution). A line-code type, used on T1 circuits, that substitutes a special code whenever 8 consecutive zeros are sent over the link. This code is then interpreted at the remote end of the connection. This technique guarantees ones density independent of the data stream. Sometimes called bipolar 8-zero substitution.

Backbone

The part of the network that carries the heaviest traffic or joins LANs together.

BER

(Bit Error Rate). Ratio of received bits that contain errors.

BIP

Bit Interleaved Parity.

Bit rate

Speed at which bits are transmitted, usually expressed in bits per second.

BITS

(Building Integrated Timing Supply). A single building master timing supply that minimizes the number of synchronization links entering an office. Sometimes referred to as a Synchronization Supply Unit.

BLSR

(Bidirectional Line Switched Ring). SONET ring architecture that provides working and protection fibers between nodes. If the working fiber between nodes is cut, traffic is automatically routed onto the protection fiber. See also *UPSR*.

Blue band

Dense Wavelength Division Multiplexing (DWDM) wavelengths are broken into two distinct bands: red and blue. DWDM cards for the ONS 15454 SDH operate on wavelengths between 1530.33nm and 1542.94nm in the blue band. The blue band is the lower frequency band.

BNC

Bayonet Neill-Concelman (coaxial cable bayonet-locking connector).

BPDU

Bridge Protocol Data Unit.

Bridge

Device that connects and passes packets between two network segments that use the same communications protocol. In general, a bridge will filter, forward, or flood an incoming frame based on the MAC address of that frame. See also *MAC address*.

Broadcast

Data packet that will be sent to all nodes on a network. Broadcasts are identified by a broadcast address. Compare with *multicast* and *unicast*. See also *Broadcast address*.

Broadcast address

Special address reserved for sending a message to all stations. Generally, a broadcast address is a MAC destination address of all ones. See also *MAC address.*

Broadcast storm

Undesirable network event in which many broadcasts are sent simultaneously across all network segments. A broadcast storm uses substantial network bandwidth and, typically, causes network time-outs.

Bus

Common physical signal path composed of wires or other media across which signals can be sent from one part of a computer to another.

C

C2 byte

The C2 byte is the signal label byte in the STS path overhead. This byte tells the equipment what the SONET payload envelope contains and how it is constructed. See also *SONET.*

CAT 5

Category 5 (cabling).

CCITT

Comité Consultatif International Télégraphique et Téléphoniques. (Formerly ITU.)

CEO

Central Office Environment.

CEV

Controlled Environment Vaults.

CLEI

Common Language Equipment Identifier code.

CLNP

Correctionless Network Protocol.

cm

Centimeter.

CMIP

Common Management Information Protocol.

COE

Central Office Environment.

Collision

In Ethernet, the result of two nodes transmitting simultaneously. The frames from each device impact and are damaged when they meet on the physical media.

Concatenation

A mechanism for allocating contiguous bandwidth for payload transport. Through the use of Concatenation Pointers, multiple OC-1s can be linked together to provide contiguous bandwidth through the network, from end to end.

CORBA

Common Object Request Broker Architecture.

CPE

Customer Premise Environments.

Crosspoint

A set of physical or logical contacts that operate together to extend the speech and signal channels in a switching network.

CTAG

(Correlation Tag). A unique identifier given to each input command by the TL1 operator. When the ONS 15454 system responds to a specific command, it includes the command’s CTAG in the reply. This eliminates discrepancies about which response corresponds to which command. See also *ATAG*.

CTC

(Cisco Transport Controller). A Java-based graphical user interface (GUI) that allows operations, administration, maintenance, and provisioning (OAM&P) of the ONS 15454 using an Internet browser.

CTM

(Cisco Transport Manager). A Java-based network management tool used to support large networks of Cisco 15000-class

D

DCC

(Data Communications Channel). Used to transport information about operation, administration, maintenance, and provisioning (OAM&P) over a SONET interface. DCC can be located in SDCC or LDCC. See also *LDCC* and *SDCC*.

DCN

Data Communications Network.

DCS

Distributed Communications System.

Default router

If the ONS 15454 must communicate with a device on a network to which the ONS 15454 is not connected, packets are sent to this router to be distributed.

Demultiplex

To separate multiple multiplexed input streams from a common physical signal back into multiple output streams. Compare *Multiplexing*.

Destination

The endpoint where traffic exits an ONS 15454 network. Endpoints can be paths (STS or STS/VT for optical card endpoints), ports (for electrical circuits, such as DS1, VT, DS3, STS), or cards (for circuits on DS1 and Ethernet cards). See also STS, and *VT*.

DRAM

Dynamic Random-Access Memory.

Drop

See *Destination*.

DS-1

Digital Signal Level One.

DS1-14

Digital Signal Level One (14 ports).

DS1N-14

Digital Signal Level One (N-14 ports).

DS-3

Digital Signal Level Three.

DS3-12

Digital Signal Level Three (12 ports).

DS3N-12

Digital Signal Level Three (N-12 ports).

DS3XM-6

Digital Service, level 3 Trans-Multiplexer 6 ports.

DSX

(Digital Signal Cross-Connect Frame). A manual bay or panel where different electrical signals are wired. A DSX permits cross-connections by patch cords and plugs.

DWDM

(Dense Wave Division Multiplexing). A technology that increases the information carrying capacity of existing fiber optic infrastructure by transmitting and receiving data on different light wavelengths. Many of these wavelengths can be combined on a single strand of fiber.

E

EDFA

(Erbium Doped Fiber Amplifier). A type of fiber optical amplifier that transmits a light signal through a section of erbium-doped fiber and amplifies the signal with a laser pump diode. EDFA is used in transmitter booster amplifiers, in-line repeating amplifiers, and in receiver preamplifiers.

EFCA

Electrical Facility Connection Assembly.

EFT

Electrical Fast Transient/Burst.

EIA

(Electrical Interface Assemblies). Provides backplane connection points for the DS-1, DS-3, and EC-1 cards.

ELR

Extended Long Reach.

EMC

Electromagnetic compatibility.

EMI

(Electromagnetic Interference). Interference by electromagnetic signals that can cause reduced data integrity and increased error rates on transmission channels.

EML

Element Manager Layer.

EMS

Element Management System.

Envelope

The part of messaging that varies in composition from one transmittal step to another. It identifies the message originator and potential recipients, documents its past, directs its subsequent movement by the Message Transfer System (MTS), and characterizes its content.

EOW

(Engineered Orderwire). A permanently connected voice circuit between selected stations for technical control purposes.

ERDI

Enhanced Remote Defect Indicator.

ES

Errored Seconds.

ESD

Electrostatic Discharge.

ESF

Extended Super Frame.

Ethernet switch

A type of Ethernet LAN device that increases aggregate LAN bandwidth by allowing simultaneous switching of packets between switch ports. Ethernet switches subdivide previously shared LAN segments into multiple networks with fewer stations per network.

ETSI

European Telecommunications Standards Institute.

Extended SNCP

(Extended Subnetwork Connection Protection). Extended SNCP extends the protection scheme of a subnetwork connection protection ring (SNCP) beyond the basic ring configuration to the meshed architecture of several interconnecting rings. See *SNCP*.

External timing reference

A timing reference obtained from a source external to the communications system, such as one of the navigation systems. Many external timing references are referenced to Coordinated Universal Time (UTC).

F

Falling threshold

A falling threshold is the counterpart to a rising threshold. When the number of occurrences drops below a falling threshold, this triggers an event to reset the rising threshold. See also *rising threshold*.

FC

Failure count.

FDDI

(Fiber Distributed Data Interface). LAN standard, defined by ANSI X3T9.5, specifying a 100-Mbps token-passing network using fiber optic cable, with transmission distances of up to 2 km. FDDI uses a dual-ring architecture to provide redundancy.

FE

Frame Bit Errors.

FG1

Frame Ground #1 (pins are labeled “FG1,” “FG2,” etc.)

FMEC

Front Mount Electrical Connection.

Frame

Logical grouping of information sent as a data link layer unit over a transmission medium. Often refers to the header and trailer, used for synchronization and error control that surrounds the user data contained in the unit.

FSB

Field Service Bulletin.

G

Gateway

An electronic repeater device that intercepts and steers electrical signals from one network to another.

GBIC

(Gigabit Interface Converter). A hot-swappable input/output device that plugs into a Gigabit Ethernet port to link the port with the fiber optic network.

Gbps

Gigabits per second.

GBps

Gigabytes per second.

GR-153-CORE

General Requirements #253 Council of Registrars.

GR-1089

General Requirements #1089.

GUI

Graphical User Interface.

H

Hard reset

The physical removal and insertion of a TCC+ card, also known as reseating a card or performing a card pull.

HDLC

(High-Level Data Link Control). Bit-oriented, synchronous, data-link layer protocol developed by ISO. HDLC specifies a data encapsulation method on synchronous serial links using frame characters and checksums.

Hop

A hop is a way to quantify the 'length' of a network route to decide which redundant route is selected. Typically each path segment through a routing network device is considered one hop. For example, if an ENE is connected to a GNE that is connected to a router, the ENE has two hops to the router—one from itself to the GNE and a second from the GNE to the router. To ensure that a certain route is used only when all other routes are exhausted, assign it an unusually high hop count.

Host number

Part of IP address used to address an individual host within the network or subnetwork.

Hot swap

The process of replacing a failed component while the rest of the system continues to function normally.

I

IEC

1. 1. InterExchange Carrier.
2. 2. International Electrotechnical Commission.

IEEE

Institute of Electrical and Electronics Engineers.

IETF

Internet Engineering Task Force.

Input alarms

Used for external sensors such as open doors, temperature sensors, flood sensors, and other environmental conditions.

I/O

Input/Output.

IP

(Internet Protocol). Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security.

IPPM

Intermediate-Path Performance Monitoring.

IP address

32-bit address assigned to host using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number.

ITU-T

International Telecommunication Union - Telecommunication Standards Sector.

J

JRE

Java Runtime Environment.

K

K bytes

Automatic protection-switching bytes located in the SONET line overhead and monitored by equipment for an indication to switch to protection.

L

LAN

(Local Area Network). High-speed, low error data network covering a relatively small geographic area. LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area. Ethernet, FDDI, and Token Ring are widely used LAN technologies.

LCD

(Liquid Crystal Display). An alphanumeric display using liquid crystal sealed between two pieces of glass. LCDs conserve electricity.

LDCC

Line Data Communication Channel.

Line layer

Refers to the segment between two SONET devices in the circuit. The line layer deals with SONET payload transport, and its functions include multiplexing and synchronization. Sometimes called a maintenance span.

Line terminating equipment (LTE)

Refers to line cards which terminate the line signal in the ONS 15454.

Line timing mode

A node that derives its clock from the SONET lines.

Link budget

The difference between the output power and receiver power of an optical signal expressed in dB. Link refers to an optical connection and all of its component parts (optical transmitters, repeaters, receivers, and cables).

Link integrity

The network communications channel has link integrity if it is intact.

Lock Out

A method of switching traffic from one card to another, or one span to another (BLSRs), that prevents traffic from reverting to the card or span with the lock out applied. The lock out overrides other manual switching connections (force, manual, and exercise).

LOF

Loss of Frame.

Loopback test

Test that sends signals then directs them back toward their source from some point along the communications path. Loopback tests are often used to test network interface usability.

LOP

Loss of Pointer.

LOS

Loss of Signal.

LOW

(Local Orderwire). A communications circuit between a technical control center and selected terminal or repeater locations.

LTE

Line Terminating Equipment.

LVDS

Low-Voltage Differential Signal.

M

MAC

Media Access Control.

MAC address

Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are six bytes long and are controlled by the IEEE. Also known as the hardware address, MAC-layer address, and physical address.

Maintenance user

A security level that limits user access to maintenance options only. See also *Superuser*, *Provisioning User*, and *Retrieve User.*

Managed device

A network node that contains an SNMP agent and resides on a managed network. Managed devices include routers, access servers, switches, bridges, hubs, computer hosts, and printers.

Managed object

In network management, a network device that can be managed by a network management protocol. Sometimes called an MIB object.

Mapping

A logical association between one set of values, such as addresses on one network, with quantities or values of another set, such as devices on another network.

Mbps

Megabits per second.

MBps

Megabytes per second.

MHz

Megahertz.

MIB

(Management Information Base). Database of network management information that is used and maintained by a network management protocol such as SNMP or CMIP. The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

MIME

Multipurpose Internet Mail Extensions.

MS

Multiplex Section.

MS-FERF

Multiplex Section Far-end Receive Failure.

MSP

Multiplex Section Protection.

MS-SPRing

(Multiplex Section Shared Protection Ring.) SDH ring architecture that provides working and protection fibers between nodes. If the working fiber between nodes is cut, traffic is automatically rerouted onto the protection fiber.

Multicast

Single packets copied by the network and sent to a specific subset of network addresses.

Multiplex payload

Generates section and line overhead, and converts electrical/optical signals when the electrical/optical card is transmitting.

Multiplexing

Scheme that allows multiple signals to be transmitted simultaneously across a single physical channel. Compare *Demultiplex*.

Mux/Demux

Multiplexer/Demultiplexer.

Muxed

Multiplexed. See *Multiplexing*.

N

NE

(Network Element). In an Operations Support System, a single piece of telecommunications equipment used to perform a function or service integral to the underlying network.

NEBS

Network Equipment-Building Systems.

NEL

Network Element Layer.

Network number

Part of an IP address that specifies the network where the host belongs.

NML

Network Management Layer.

NMS

(Network Management System). System that executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management.

Node

Endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be processors, controllers, or workstations. Nodes, which vary in routing and other functional capabilities, can be interconnected by links, and serve as control points in the network. Node is sometimes used generically to refer to any entity that can access a network. In this manual the term “node” usually refers to an ONS 15454.

O

OAM&P

(Operations, Administration, Maintenance, and Provisioning). Provides the facilities and personnel required to manage a network.

OC

Optical carrier.

OOS AS

Out of Service Assigned.

Optical amplifier

A device that amplifies an optical signal without converting the signal from optical to electrical and back again to optical energy.

Optical receiver

An opto-electric circuit that detects incoming lightwave signals and converts them to the appropriate signal for processing by the receiving device.

Orderwire

Equipment that establishes voice contact between a central office and carrier repeater locations. See *Local orderwire*.

OSI

Open Systems Interconnection.

OSPF

Open Shortest Path First.

OSS

Operations Support System.

OSS/NMS

Operations Support System/Network Management System.

Output contacts (controls)

Triggers that drive visual or audible devices such as bells and lights. Output contacts can control other devices such as generators, heaters, and fans.

P

Passive devices

Components that do not require external power to manipulate or react to electronic output. Passive devices include capacitors, resisters, and coils.

Path Layer

The segment between the originating equipment and the terminating equipment. This path segment may encompass several consecutive line segments or segments between two SONET devices.

Payload

Portion of a cell, frame, or packet that contains upper-layer information (data).

PCM

Pulse Code Modulation.

PCMCIA

Personal Computer Memory Card International Association.

PCN

Product Change Notice(s).

PDI-P

STS Payload Defect Indication - Path.

Ping

(Packet internet grouper). ICMP echo message and its reply. Often used in IP networks to test the reachability of a network device.

Pointer justification

In SONET, the mechanism used to compensate for frequency and phase variations. Pointer justification counts indicate timing errors on SONET networks.

POP

Point of Presence.

PM

Performance Monitoring.

PPMN

(Path-Protected Mesh Network). PPMN extends the protection scheme of a unidirectional path switched ring (UPSR) beyond the basic ring configuration to the meshed architecture of several interconnecting rings.

Priority queuing

Routing feature that divides data packets into two queues: one low-priority and one high-priority.

Protect card

A card in a protection pair or scheme that is provisioned as a protect card to the working card. If the working card fails, the protect card becomes active. See also *working card*.

Provisioning user

A security level that allows the user to access only provisioning and maintenance options in CTC. See also *Superuser*, *Maintenance user,* and *Retrieve user*.

PSC

Protection-Switching Count.

PSD

Protection-Switching Duration.

PTE

Path-Terminating Equipment.

Q

Queue

In routing, a backlog of packets waiting to be forwarded over a router interface.

R

RAM

Random Access Memory.

RDI-L

Remote Defect Indication - Line.

Red band

DWDM wavelengths are broken into two distinct bands: red and blue. The red band is the higher frequency band. The red band DWDM cards for the ONS 15454 SDH operate on wavelengths between 1547.72nm and 1560.61nm.

RES

Reserved.

Retrieve user

A security level that allows the user to retrieve and view CTC information but not set or modify parameters. See also *Superuser*, *Maintenance user*, and *Provisioning user*.

Revertive switching

A process that sends electrical interfaces (traffic) back to the original working card after the card comes back online.

Rising threshold

The number of occurrences (collisions) that must be exceeded to trigger an event.

RJ-45

Registered Jack #45 (8-pin).

RMA

Return Materials Authorization.

RMON

(Remote Network Monitoring). Allows network operators to monitor the health of the network with a Network Management System (NMS). RMON watches several variables, such as Ethernet collisions, and triggers an event when a variable crosses a threshold in the specified time interval.

RS-232

Recommended Standard #232 (ANSI Electrical Interface for Serial Communication).

Rx

Receive.

S

SCI

Serial Communication Interface.

SCL

System Communications Link.

SDCC

Section Data Communication Channel.

SDH

(Synchronous Digital Hierarchy). European standard that defines a set of rate and format standards that are transmitted using optical signals over fiber. SDH is similar to SONET, with a basic SDH rate of 155.52 Mbps. Compare *SONET.*

SEF

Severely Errored Frame.

SELV

Safety Extra-Low Voltage.

SES

Severely Errored Seconds.

SF

Super Frame.

SML

Service Management Layer.

SMF

Single Mode Fiber.

SNCP

(Subnetwork Connection Protection Ring). Path-switched SDH rings that employ redundant, fiber-optic transmission facilities in a pair configuration. One fiber transmits in one direction and the backup fiber transmits in the other. If the primary ring fails, the backup takes over.

SNMP

(Simple Network Management Protocol). Network management protocol used almost exclusively in TCP/IP networks. SNMP monitors and controls network devices and manages configurations, statistics collection, performance, and security.

SNTP

(Simple Network Time Protocol). Using an SNTP server ensures that all ONS 15454 network nodes use the same date and time reference. The server synchronizes alarm timing during power outages or software upgrades.

Soft reset

A soft reset reloads the operating system, application software, etc., and reboots the TCC+ card. It does not initialize the ONS 15454 ASIC hardware.

SONET

(Synchronous Optical Network). High-speed synchronous network specification developed by Telcordia Technologies, Inc. and designed to run on optical fiber. STS-1 is the basic building block of SONET. Approved as an international standard in 1988.

Source

The endpoint where traffic enters an ONS 15454 network. Endpoints can be a path (STS or STS/VT for optical card endpoints), port (for electrical circuits, such as DS1, VT, DS3, STS), or card (for circuits on DS1 and Ethernet cards). See also *STS* and *VT*.

Span

An optical path between two nodes.

Spanning tree

A loop-free subset of a network topology. See also *STA* and *STP*.

SPE

(Synchronous Payload Envelope). A SONET term describing the envelope that carries the user data or payload.

SSM

(Synchronous Status Messaging). A SONET protocol that communicates information about the quality of the timing source using the S1 byte of the line overhead.

STA

(Spanning-Tree Algorithm). An algorithm used by the spanning tree protocol to create a spanning tree. See also *Spanning tree* and *STP*.

Standby card

A card that is not active or carrying traffic. A standby card can be a protect card or, after a protection switch, a working card can be a standby card.

Static route

A route that is manually entered into a routing table. Static routes take precedence over routes chosen by all dynamic routing protocols.

STP

1. 1. Shielded Twisted Pair.
2. 2. Spanning Tree Protocol. Bridge protocol that uses the spanning-tree algorithm to enable a learning bridge to dynamically work around loops in a network topology by creating a spanning tree. See also *Spanning tree and STA*.

STS

(Synchronous Transport Signal, used generically when speaking of SONET signals.)

STS-1

(Synchronous Transport Signal Level 1). Basic building block signal of SONET, operating at 51.84 Mbps for transmission over OC-1 fiber. Faster SONET rates are defined as STS-*n*, where *n* is a multiple of 51.84 Mbps. See also *SONET*.

Subnet mask

32-bit address mask used in IP to indicate the bits of an IP address that are used for the subnet address. Sometimes referred to simply as mask. See also *IP address mask* and *IP address*.

Subnetwork

In IP networks, a network confined to a particular subnet address. Subnetworks are networks segmented by a network administrator in order to provide a multilevel, hierarchical routing structure while shielding the subnetwork from the addressing complexity of attached networks. Sometimes called a subnet.

Subtending rings

SONET rings that incorporate nodes that are also part of an adjacent SONET ring.

Superuser

A security level that can perform all of the functions of the other security levels as well as set names, passwords, and security levels for other users. A superuser is usually the network element administrator. See also *Retrieve user*, *Maintenance user*, and *Provisioning user.*

Switching, Span

Span switching occurs when a working span fails. Traffic switches to the protect fibers between the nodes and then returns to the working fibers. Multiple span switches can occur at the same time.

Switching, Ring

Ring switching occurs when a span switch cannot recover traffic, such as when both the working and protect fibers fail on the same span. In a ring switch, traffic is routed to the protect fibers throughout the full ring.

SWS

SONET WAN switch.

SXC

SONET Cross Connect ASIC.

T

T1

T1 transmits DS-1-formatted data at 1.544 Mbps through the telephone-switching network using AMI or B8ZS coding. See also *AMI*, *B8ZS*, and *DS-1*.

TAC

Technical Assistance Center.

Tag

Identification information, including a number plus other information.

TBOS

Telemetry Byte-Oriented Serial protocol.

TCA

Threshold Crossing Alert.

TCC+

Timing Communications and Control + Card

TCP/IP

Transmission Control Protocol/Internet Protocol

TDM

(Time Division Multiplexing). Allocates bandwidth on a single wire for information from multiple channels based on preassigned time slots. Bandwidth is allocated to each channel regardless of whether the station has data to transmit.

TDS

Time-Division Switching.

Telcordia

(Telcordia Technologies, Inc., formerly named Bellcore). Eighty percent of the U.S. telecommunications network depends on software invented, developed, implemented, or maintained by Telcordia.

TID

(Target Identifier). Identifies the particular network element (in this case, the ONS 15454) where each TL1 command is directed. The TID is a unique name given to each system at installation. See also *AID*.

TL1

Transaction Language 1.

TLS

(Transparent LAN Service). Provides private network service across a SONET backbone.

TMN

Telecommunications Management Network.

Transponder

Optional devices of a DWDM system providing the conversion of one optical wavelength to a precision narrow band wavelength. See also *DWDM*.

Trap

Message sent by an SNMP agent to an NMS (CTM), console, or terminal to indicate the occurrence of a significant event, such as an exceeded threshold. See also *CTM*.

Tributary

The lower-rate signal directed into a multiplexer for combination (multiplexing) with other low rate signals to form an aggregate higher rate level.

Trunk

Network traffic travels across this physical and logical connection between two switches. A backbone is composed of a number of trunks. See also *Backbone*.

TSA

Time-Slot Assignment.

TSI

Time-Slot Interchange.

Tunneling

Architecture that is designed to provide the services necessary to implement any standard point-to-point encapsulation scheme.

Tx

Transmit.

U

UAS

Unavailable Seconds.

UDP/IP

User Datagram Protocol/Internet Protocol.

UID

User Identifier.

Unicast

The communication of a single source to a single destination.

UPSR

(Unidirectional Path Switched Ring). Path-switched SONET rings that employ redundant, fiber- optic transmission facilities in a pair configuration. One fiber transmits in one direction and the backup fiber transmits in the other. If the primary ring fails, the backup takes over. See also *BLSR*.

Upstream

Set of frequencies used to send data from a subscriber to the head end.

UTC

Universal-Time Coordinated.

UTP

Unshielded Twisted Pair.

V

VDC

Volts Direct Current.

Virtual fiber

A fiber that carries signals at different rates and uses the same fiber optic cable.

Virtual ring

Entity in a source-route bridging (SRB) network that logically connects two or more physical rings together either locally or remotely. The concept of virtual rings can be expanded across router boundaries.

Virtual wires

Virtual wires route external alarms to one or more alarm collection centers across the SONET transport network.

VLAN

(Virtual LAN). Group of devices located on a number of different LAN segments that are configured (using management software) to communicate as if they were attached to the same wire. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VPN

(Virtual Private Network). Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level. See also *Tunneling*.

VT

(Virtual Tributary). A structure designed for the transport and switching of sub-DS3 payloads. See also *Tributary.*

VT1.5

Virtual Tributary that equals 1.544 Mbps.

VT layer

The VT layer or electrical layer occurs when the SONET signal is broken down into an electrical signal.

VT tunnel

VT tunnels allow electrical circuits to pass through ONS 15454 nodes without using ONS 15454 cross-connect card capacity.

W

W

Watts.

WAN

Wide Area Network.

Working card

A card that is provisioned as an active, primary card. Traffic cards in a protection pair are provisioned as working or protect See also *Protect card*.

X

XC

Cross Connect

XCVT

Cross Connect Virtual Tributary.

X.25

Protocol providing devices with direct connections to a packet-switched network.

INDEX

Numerics

- 1+1 optical card protection
  - apply a force switch 11-9
  - delete 10-14
  - modify 10-13
  - summary GL-1
  - test 4-8
  - upgrade optical speeds 11-3, 11-6, 11-9
  - verify active/ standby status for a port 12-5
- 1:1 electrical card protection
  - description GL-1
- 1:1 electrical port protection 3-20
- 1:N electrical card protection
  - description GL-1
- 100 Base T GL-1
- 100 Base TX GL-1
- 10 Base T GL-1

A

- access drop GL-1
- access identifier (TL1) GL-2
- active (definition) GL-1
- add/ drop multiplexer *see* linear ADM
- add node
  - to a BLSR 13-2
  - to a current session 2-26
  - to a domain 10-10
  - update circuits with new node A-7
  - UPSR 13-13
- ADM *see* linear ADM
- agent GL-2
- AID GL-2
- air filter
  - location 1-20
  - replace (disposable) 14-4
  - replace (reusable) 14-2
  - requirement 1-20
- AIS GL-2
- AIS threshold
  - change timing source 10-16
  - external or line timing 3-18
- alarm indication signal *see* AIS
- alarm profiles
  - create 6-16
  - apply to ports 6-20
  - assign to cards and nodes 6-23
  - delete 6-24
  - download 6-19
- alarms
  - severity profiles *see* alarm profiles
  - delete cleared alarms from display 6-12
  - display 6-5
  - Ethernet RMON alarm thresholds 3-23, 10-25
  - history 6-7, 6-9
  - raise (unsuppress) 6-31
  - suppress 6-29
  - synchronize 6-10
  - troubleshoot *see Cisco ONS 15327 Troubleshooting Guide*
- alarm severities *see* alarm profiles
- alarm wires 1-29
- AMI 3-18, GL-2
- area range table (OSPF) 3-11
- ATM GL-3

automatic host detection 2-15

automatic protection switching

- bidirectional switching 3-21
- count 9-13
- definition GL-2
- duration 9-13
- inhibit 14-16
- revertive switching 3-21, 5-25

auto-ranging 5-5, 5-16, 5-35

AWG wire 1-13

B

B8ZS 3-18, GL-3

backbone GL-3

bandwidth B-1

bit error rate (BER) GL-3

BITS

- BITS out references 3-18, 10-16
- definition GL-3
- external timing pin assignments 1-32
- facilities 3-18, 10-16
- interface specifications B-3
- pin assignments 1-31
- timing setup 3-17

blade *see* card

BLSR

- acceptance test 4-16
- add a node 13-2, 13-6
- choose properties 4-14
- definition GL-3
- delete a node from a ring 13-12
- disable the ring 13-12
- drop a node 13-9
- exercise the ring 4-18
- install fiber 1-46
- modify ring ID, node ID, or ring reversion 12-8
- remove a node 13-9
- subtend a BLSR 4-27
- subtend a UPSR 4-25
- upgrade optical speeds 11-6
- verify fiber connections 4-13
- verify timing after dropping a node 13-12

bridge GL-4

broadcast

- address GL-4
- storm GL-4

bus GL-4

C

C2 byte GL-4

cable

- patch *see* patch cables
- CAT-5 *see* LAN cable
- connect PC to ONS 15327 2-13
- DS-1 *see* DS-1 cable
- route through fiber-optic cable storage drawer D-2

cable storage drawer D-2

card protection

- *see* 1+1 optical card protection
- *see* 1:1 electrical port protection 3-20

card protection *see* 1:1 electrical card protection

card provisioning

- electrical cards 9-1
- optical cards 9-9

cards

- protection *see* card protection
- active GL-1
- delete 1-26
- line terminating cards 7-2
- list B-1
- part number A-8
- put ports in/ out of service 4-5
- remove and replace 1-26
- reseat GL-10
- reset the XTC 14-23
- revision number A-8

serial number A-8
standby GL-20
upgrades 11-1
verify installation 3-2
working GL-24
CARLOSS 5-62
CAT-5 cable *see* LAN cable
circuits
see also cross-connect
see also electrical circuits
see also Ethernet
see also optical circuits
add a node A-7
auto-range 5-5
convert a CTC circuit to TL1 cross-connects 8-11
delete 8-13
destination 5-2, GL-6
downgrade a circuit 8-11
edit name 8-8
edit UPSR circuits 8-10
fully-protected path 5-7
locate and view 8-3
make an upgradeable circuit active 8-13
monitor 8-14
multiple drops 5-11, 5-22, 5-41
node name change 14-10
provision UPSR path selectors 5-25
provision with a shortcut A-7
repair a missing cross-connect 8-11
search 8-5
source 5-2
source (definition) GL-20
STS source and destination options 5-3
upgrade a span A-7
upgrade TL1 cross-connects to a CTC circuit 8-13
UPSR path selectors 5-39
view alarms on circuits 6-13
VT source and destination options 5-2
Cisco Transport Controller *see* CTC
CLEI code A-8
clock
change time 10-3
set time 3-6
coaxial cable
BNC connectors 1-38
high-density BNC connectors 1-40
collision GL-5
concatenation GL-5
conditions 6-11
configurations *see* networks
connection methods 2-8
contact 3-5
CORBA 3-14
corporate LAN 2-9, 2-19
cost 3-9, 3-10, 10-6
craft access 3-8
craft connection 2-9
cross-connect (circuit)
convert a circuit into TL1 cross connects 8-11
definition 5-57
E series multicard EtherSwitch 5-60
E series single-card EtherSwitch 5-57
G1000-2 5-70
replace a missing cross-connect 8-11
see circuits
upgrade TL1 cross-connects to a CTC circuit 8-13
crosspoint GL-5
CTAG GL-5
CTC
see also PC setup 2-2
toolbar icons *see* toolbar icons
back up 14-6
card protection setup 3-20
connect PCs 2-8
export data 6-3
firewall access 3-13
installation wizard (UNIX) 2-5
installation wizard (Windows) 2-2

log in 2-22
login node groups 2-25
node setup 3-5
online documentation 2-2, 2-5
PC requirements 2-2
print data 6-2
remote site access 2-21, 2-22
revert to earlier load 14-19
timing setup 3-16, 10-15
UNIX workstation requirements 2-5
views *see* views
CTM GL-6
CV parameter, provisioning 9-12

D

database
back up 14-6
Cisco recommendation for separate folders 14-10
clear the database 14-10
parameters that are not restored 14-10
restore node and card defaults during disaster recovery 14-10
restore the database 14-8
revert to earlier software database 14-19
data communications channel *see* DCC
date
change setting 10-3
provision 3-6
DCC
create DCC terminations 4-4
create DCC tunnel 5-75
delete DCC terminations 10-14
delete DCC tunnel 10-14
disable autodiscovery 2-24
metric (OSPF) 3-10
OSPF Area ID 3-10
terminations, definition GL-6
default router
change in CTC 10-5
definition GL-6
enter IP address 3-8
initially provision 3-7
demultiplex GL-6
destination GL-6
DHCP 2-13
change request receipient 10-5
enable 3-8
provision server 3-7
DNS configuration 2-11, 2-13, 2-15, 2-19
domains
create 10-10
open 10-11
remove 10-11
rename 10-11
drops
access drop GL-1
definition GL-6
drop port in path trace 8-17
LTE 7-2
multiple drops on a DS-1 circuit 5-11
multiple drops on a DS-3 circuit 5-22
multiple drops on an optical circuit 5-41
protected drops 5-6
DS-1 cable
install 1-33
install Champ cables on a MIC 1-34
right-angle 1-34, 1-37
screw-lock power connector 1-14
straight 1-34, 1-36, 1-38
DS-1 circuits *see* electrical circuits
DS-3 circuits *see* electrical circuits
DWDM
blue band GL-4
definition GL-7
EDFA GL-7
transponder GL-22
dynamic host configuration protocol *see* DHCP

E

east *see* fiber connections

electrical cable *see* coaxial cable

electrical cards

- circuit types *see* electrical circuits
- circuit source and destination options 5-2
- *see* XTC card

electrical circuits

- DS-1, automatically routed 5-5
- DS-1, manually routed 5-9
- DS-1, multiple drops 5-11
- DS-3, automatically routed 5-16
- DS-3, manually routed 5-20
- DS-3, multiple drops 5-22

EMI GL-8

enterprise LAN *see* corporate LAN

environment variable 2-7

equipment

- cards *see card names*
- installation 1-2

E-Series cards

- *see also* Ethernet
- MAC address table 14-26
- spanning tree parameters 14-25

ES parameter, provision 9-12

Ethernet

- circuits 5-48 to 5-74
- create a G-series circuit 5-68
- delete RMON alarm thresholds 10-25
- E series multicard EtherSwitch manual cross-connect 5-60
- E-Series port-mapped circuit 5-50
- E series shared packed ring circuit 5-52
- E series single-card EtherSwitch manual cross-connect 5-57
- hub-and-spoke circuit 5-55
- provision E-series ports 5-64
- provision G-series ports 5-72
- provision ports for VLAN membership 5-65
- route fiber 1-47
- *see also* G-Series cards
- switch (definition) GL-8
- test circuits 5-67
- threshold variables (MIBs) 3-24

Ethernet cards

- *see also* G-Series cards
- *see* circuits
- *see* E-Series cards
- *see* Ethernet

exercise ring 4-18

export 6-3

express orderwire see orderwire

external alarms *see* XTC card

external controls *see* XTC card

external switching commands

- apply a lock on 14-16
- BLSR ring switch test 4-19
- card lockout 14-17
- clear a BLSR Force ring switch 13-8
- clear a BLSR Manual ring switch 12-10
- clear a lock on 14-18
- initiate a BLSR Force ring switch 13-6
- initiate a BLSR Manual ring switch 12-9
- initiate a UPSR Force switch 13-16
- lock on 14-16
- lock out 14-17
- UPSR span switch test 4-25

external timing reference see timing

F

factory configuration *see* network element defaults

failure count, provisioning 9-13

falling threshold GL-9

fan-tray air filter *see* air filter

fan-tray assembly 1-20

fiber

attach to OC-N cards 1-42

BLSR configuration 1-46

cable storage drawer D-2

clean connectors 14-20, 14-21

connection guidelines 1-46

route cable through cable storage drawer D-2

route through cable guides 1-47

scope and clean adapters 14-21

scope and clean connectors 14-21

UPSR configuration 1-43

fiber connections

subtend a BLSR from a USPR 4-27

subtend a UPSR from a BLSR 4-25

verify UPSR 4-22

firewalls 3-8, 3-13

force switch *see* external switching commands

framing 3-18, 10-16

fuse and alarm panel

location 1-9

measure and cut cables 1-15, D-5

verify installation 1-8, 1-9, 1-13

G

G-10002 card *see* G-series cards

gateway GL-9

gateway settings 3-8, 10-5

glossary GL-1

ground 1-12, 1-13

G-Series cards

see also Ethernet

bandwidth usage 14-25

create a G-Series circuit 5-68

create a manal cross-connect in port-mapped mode 5-70

install SFPs 1-24

loopback status 14-24

manual cross-connect 5-70

H

hard reset GL-10, GL-11

hardware redundancy test *see* XTC card

hello interval 3-11

hop 3-9, 10-6

hub-and-spoke 5-55

I

idle time 3-4, 3-5

IIOP 3-13

listener port 3-7, 3-14, 10-5

select IIOP listener port 3-8

installation

19-inch rack 1-6

empty shelf 1-5

power supply 1-12

reversible mounting bracket 1-6

tools 1-2

installation wizard (UNIX) 2-5

installation wizard (Windows) 2-2

interface *see* ports

intermediate-path performance monitoring *see* IPPM

Internet Explorer

disable proxy service 2-20

log in 2-23

Internet Inter-ORB Protocol *see* IIOP

inventory A-8

IP address

host number GL-10

initial configuration 2-11, 2-15, 2-16, 2-17

NMS 3-21

select IP address for log in 2-24

set up network information 3-8

IPPM

definitions 7-5

enable 7-4

monitored IPPMs 7-4

purpose 7-4

J

J1 path trace
provision on circuit source and destination 8-16
provision on OC-N ports 8-19
java runtime environment *see* JRE
JRE
install (Solaris) 2-6
install (Windows) 2-4
java.policy file 2-2, 2-4
modify policy file (Solaris) 2-6
modify policy file (Windows) 2-4
patches 2-7
reference 2-8

K

K byte GL-11

L

LAN
cable *see* LAN cable
connection point *see* XTC card
definition GL-11
modems 2-21
OSPF activity 3-10
set up OSPF 3-7
LAN cable 2-13
automatic host detection 2-15
connect computer to RJ-45 2-22
crimp 2-23
latitude 3-5
LGX 1-42
linear ADM
acceptance test 4-11
definition GL-2
provision 4-10
upgrade to a two-fiber BLSR 12-3
upgrade to a UPSR 12-6
line terminating equipment 7-2
link budget GL-12
listener port 3-14
log in 2-22
login node groups
create 2-25
view 2-24
longitude 3-5
loopback
see also the Cisco ONS 15327 Troubleshooting Guide
BLSR 4-17
definition GL-12
linear ADM 4-12
point-to-point 4-7
UPSR 4-24

M

MAC address
definition GL-13
location 3-8
managed device GL-13
managed object GL-13
map (network) 10-8, 10-9
memory B-3
MIB 3-24, GL-13
modem interface B-2
module *see* card
monitor circuits 8-14
monitoring, peformance *see* performance monitoring
mounting brackets 1-6
multicast GL-14
multiple drops *see* circuits
multiplex GL-14
muxed see multiplex

N

Netscape Communicator 2-3, 2-6

Netscape Navigator

- disable proxy service 2-20
- log in 2-23
- testing the node connection 2-18

network element

- definition GL-14
- see node

network element defaults

- card settings C-4 to C-13
- description C-1
- edit C-2
- export defaults to other nodes C-4
- import from a CD or file C-3
- node settings C-14
- overview C-1
- restore during disaster recovery 14-10

networks

- point-to-point *see* point-to-point
- BLSR *see* BLSR
- building circuits 5-1, 8-1
- default configuration *see* UPSR
- linear ADM *see* linear ADM
- set up basic information 3-7
- verify network turn up 5-3

network time protocol 3-6

network view

- add nodes to map *see* domains
- apply a custom background image (map) 10-9
- change the background color 10-8
- change the default network map 10-8
- create new users 3-3, 3-4
- delete users 10-23
- display a link end (drop) point A-7
- tasks A-6
- update circuits with new node A-7
- upgrade a span A-7

node

- add to current session 2-26
- change node name 10-2
- date, time, and contact information 3-5
- definition GL-15
- remove power 15-1
- turn up 3-1 to 3-26

node maintenance 14-1 to 14-28

node view

- alarm profiles, assign 6-23
- create users 3-3
- setting up timing 10-15
- set up basic network information 3-7
- set up timing 3-17

NPJC-Pdet parameter 9-13

NPJC-Pgen parameter 9-13

NTP 3-6

O

OC-N cards

- attach fiber 1-42
- attenuation 1-40
- BLSR trunk cards 4-13
- modify thresholds 9-11
- provision line transmission settings 9-9
- route fiber 1-47
- set port to SDH 9-14
- upgrading to a higher rate while in-service 11-5
- verify installation 3-2

office ground 1-13

office power 1-14, 1-19, D-4

online documentation

- UNIX 2-5
- Windows 2-2

optical (STS) circuits

- automatically routed 5-35
- manually routed 5-38
- multiple drops 5-41

test 5-46

optical cards *see* OC-N cards

optical transmit and receive levels 1-41

orderwire

EOW (definition) GL-8

OSPF

area range table 3-11

DCC OSPF area 3-10

disable 10-7

intervals 3-11

LAN activity 3-10

priority level 3-11

set up or change 3-10

output contacts see AIC card, external controls

P

passwords

create new user 3-4

login 2-24

modify 10-19, 10-20

patch cables

BLSR test 4-17

linear ADM test 4-12

point-to-point test 4-6

USPR test 4-24

path layer GL-16

path see spans

path trace *see* J1 path trace 8-19

PC

see also set up PC

connect to ONS 15327 using a craft connection 2-9

PC setup

install browser 2-2

install JRE 2-2

modify java.policy file 2-2

requirements 2-2

performance monitoring 7-1 to 7-19

15-minute intervals 7-8

clear count selected 7-11

display PMs 7-7, 7-13

Ethernet 3-23

intermediate-path performance monitoring *see* IPPM

monitor far-end counts 7-10

monitor near-end counts 7-10

monitor selected signal type counts 7-14

pointer justification counts *see* pointer justification counts

refresh counts 7-8, 7-9, 7-18

reset (baseline) counts 7-11

set auto-refresh 7-12

threshold crossing alert *see* TCA

ping GL-16

pointer justification GL-16

pointer justification counts

enable 7-2

purpose 7-2

point-to-point

acceptance test 4-6

prerequisites 4-3

provision 4-3

upgrade to a linear ADM 12-1

upgrade to a two-fiber BLSR 12-3

upgrade to a UPSR 12-6

port filtering 3-13

ports

change OC-N port to SDH 9-14

default UDP port for SNMP 10-24

E-series Ethernet 5-64

G-Series Ethernet 5-72

listener port 3-14

provision for 1+1 protection 3-20

put optical ports in/ out of service 4-5

UDP 3-21

power

connect office power to shelf 1-14, D-4

measure voltage 1-49

power down a node 15-1

specifications B-3
supply 1-12
verify office power 1-19
PPJC-Pdet parameter 9-13
PPJC-Pgen parameter 9-13
priority queuing GL-17
procedures
for procedures organized by chapter, see the list of procedures at the front of the book
alarm-affected circuits, view 6-13
alarms, delete 6-12
alarm severity profiles, create and assign 6-15
automatically-routed DS-1 circuit, create 5-5
automatically-routed DS-3 circuit, create 5-16
automatically-routed optical circuit, create 5-35
BLSR, acceptance test 4-16
BLSR, create 4-14
BLSR, subtend from a BLSR 4-27
BLSR node, add 13-2
BLSR noded, remove 13-9
BLSR nodes, provision 4-13
BLSR ring ID, node ID, and ring reversion, modify 12-8
card installation, verify 3-2
card protection, change settings 10-12
circuit characteristics, modify 8-7
circuits, delete 8-13
circuits, locate and view 8-3
clear the database and upload software (UNIX) 14-13
clear the database and upload software (Windows) 14-11
conditions, view 6-5
CTC network access, change 10-4
CTC network access, provision 3-7
CTC network view, customize 10-7
database, back up 14-6
database, restore 14-8
DCC tunnel, create 5-75
earlier software load, revert 14-19
electrical cable, install 1-33
electrical cable, route 1-39
electrical circuits, test 5-33
E series Ethernet circuits, test 5-67
Ethernet RMON alarm thresholds, create 3-23
events, view 6-5
existing provisioning, document 6-2
factory configuration, restore 14-10
fan-tray assembly, install 1-20
fiber connectors, clean 14-20
firewall access, set up 3-13
G series circuits, test 5-73
J1 path trace, create 8-15
linear ADM, acceptance test 4-11
linear ADM, provision 4-10
linear ADM, upgrade to two-fiber BLSR 12-3
linear ADM, upgrade to UPSR 12-6
log into the ONS 15327 GUI 2-22
manually-routed DS-1 circuit, create 5-9
manually-routed DS-3 circuit, create 5-20
manually-routed optical circuit, create 5-38
monitor circuit, create 8-14
network turn up, acceptance test 5-3
node information, set up 3-5
node management information, change 10-2
optical circuits, test 5-46
optical spans, upgrade automatically 11-3
optical spans, upgrade manually 11-5
path trace, create 8-15
performance, monitor 7-6, 7-15
performance monitoring, enable 7-2
point-to-point, acceptance test 4-6
point-to-point network, upgrade to linear ADM 12-1
point-to-point network, upgrade to two-fiber BLSR 12-3
point-to-point network, upgrade to UPSR 12-6
power and ground, install 1-12
protection groups, create 3-20
protection switching, inhibit 14-16
reset, soft 14-23

security, assign 3-3
security, modify 10-17
shelf assembly, acceptance test 1-48
shelf assembly, install 1-5
shelf assembly, power down 15-1
shelf assembly, unpack 1-4
shelf assembly, verify installation 4-2
SNMP, set up 3-21
SNMP settings, change 10-23
terminal point-to-point network, provision 4-3
timing, change 10-15
timing, set up 3-16
unidirectional DS-1 circuit with multiple drops, create 5-11
unidirectional DS-3 circuit with multiple drops, create 5-22
unidirectional optical circuit with multiple drops, create 5-41
UPSR, acceptance test 4-23
UPSR, subtend from a BLSR 4-25
UPSR, upgrade to BLSR 12-6
UPSR node, add 13-13
UPSR node, remove 13-15
UPSR nodes, provision 4-22
users, create 3-3
users, modify 10-17
VT tunnel, create 5-28, 5-30
XTC, reset using CTC 14-23

protection
see automatic protection switching
see card protection

protocols
DHCP 3-8
NTP 3-6
SNTP 3-6

proxy server features 3-8

proxy service 2-20

PSC parameter
provisioning 9-13
provisioning PSC-W 9-13

PSD parameter
provisioning PSD-L 9-13
provisioning PSD-W 9-13

Q

queue GL-17

R

rack
mount a shelf 1-8
mount multiple shelves 1-8

rack installation
19-inch rack 1-6
reversible mounting bracket 1-6

RAM, PC requirements for CTC 2-2

reinitialization tool 14-10

remote network monitoring GL-18

reset 14-23

restore the node to factory configuration 14-10

revert 14-19

revertive timing 3-17

rings
see BLSR
see subtending rings
see UPSR

RIP 3-12

rising threshold GL-18

RJ-45
pins 1-30
see also BITS, pin assignnments
see also XTC card

RMON GL-18

RX levels 1-41

S

SC connector *see also* cable

SD BER, provisioning 9-10

SDH 9-14

security

- modify settings 10-17
- set up 3-3

SEFS parameter 9-13

SES parameter, provisioning 9-12

set up PC

- connect cable to ONS 15327 2-22
- connection to ONS 15327 2-1
- corporate LAN connection 2-19
- craft connection (requiring IP address reconfiguration 2-11
- craft connection (without multiple IP reconfigurations) 2-15
- craft connection using DHCP 2-13
- disable proxy service 2-20
- remote (modem) access 2-21

SF BER parameter, provisioning 9-10

SFP connectors

- install 1-24
- remove 1-25

shared packet ring 5-52

shelf

- acceptance test 1-48
- airspace requirement 1-6
- change contact information 10-2
- connect office power 1-14, D-4
- connect the office ground 1-13
- dimensions B-3
- environmental specifications B-3
- inspect 1-5
- install 1-1
- mounting 1-8
- specifications B-1
- temperature warning 1-5
- turn up 3-1 to 3-24
- unpack 1-4

shells 2-8

simple network time protocol *see* SNTP

slots

- assignments B-1
- verify that a 1+1 working slot is active 12-5

small-form factor plugabbles *see*SFP connectors

SNMP 3-21

- delete Ethernet RMON alarm thresholds 10-25
- delete trap destination 10-25
- modify trap destination 10-24
- UDP port 10-24

SNTP 3-6

software

- *see also* CTC
- determine version 2-23
- incompatible alarm 2-23
- install CD-ROM 2-2
- revert 14-19
- set up 2-1
- version mismatch among multiple nodes 2-23

Solaris

- connect cable to ONS 15327 2-22
- CTC set up 2-7
- disable proxy service 2-20
- installation wizard 2-5
- set up craft connection to ONS 15327 2-17
- set up JRE 2-7

SONET DCC *see* DCC

spanning tree GL-20

spans

- change color 8-9
- definition GL-20
- display span information A-5
- switching (UPSR) 4-25
- upgrade alarms 11-5
- upgrade hardware compatibility 11-6
- upgrade optical spans 11-3

upgrades 11-1
view circuits on a span 8-6
view properties A-7
span upgrade wizard 11-3
SSM
enable 3-18, 9-10, 10-16
message set 3-17, 10-16
standard constant 3-15
static route
create 3-9
delete 10-6
modify 10-6
straight-through (CAT-5) cable *see* LAN cable
STS *see* optical circuits
subnet mask GL-20
change 10-5
OSPF area range table 3-11
provision 3-7
provision in a static route 3-9
provision subnet mask length 3-8
Windows setup 2-12
subtending rings
subtend a BLSR from a BLSR 4-27
subtend a BLSR from a UPSR 4-27
subtend a UPSR from a BLSR 4-25
switching
see automatic protection switching
see external switching commands
system *see* networks

T

tables
see also List of Tables
change format A-7
display hidden columns A-7
print data 6-2
resize columns A-7
sort A-7
TCA 7-8
15-minute interval 7-8
1-day interval 7-9
TCP/ IP 2-11, 2-13, 2-15
TDM GL-22
Telcordia
performance monitoring 7-1
timing requirements B-3
temperature 1-5
terminal system *see* point-to-point
threshold crossing alert *see* TCA
thresholds
DS-1 card 9-2
DS-3 card 9-6
Ethernet 3-23
optical cards 9-11
time division multiplexing GL-22
timed out *see* idle time
time zone 3-6, 10-3
timezone 6-10
timing
BITS *see* BITS
change timing source 10-15
external 3-17
external timing (definition) GL-9
internal 3-19
line 3-17
mode 3-18
NE reference 3-18
select reversion time 10-16
set node clock 3-6
set up 3-17
specifications B-3
verify timing in a reduced ring 13-12
timing wires 1-30
TL1
AID definition GL-2
ATAG GL-3
craft interface connection 1-32

interface specifications B-2
toolbar icon A-4
toolbar icons
add node A-2
export A-2
go to home view A-3
go to network view A-3
go to next view A-3
go to parent view A-3
go to previous view A-3
go to selected object view A-3
lock node A-2
open TL1 connection A-4
preferences A-3
print A-2
tools (equipment) 1-2
topology hosts 2-24
traffic
see also circuits
cards *see also* OC-N cards
traffic monitoring
see also performance monitoring
create monitor circuits 8-14
create path trace 8-15
provision J1 path trace on OC-N ports 8-19
trap 3-22, GL-22
tributary GL-22
trunk GL-22
TX levels 1-41

U

UAS parameter 9-13
unpack 1-4
upgrade
cards 11-1
optical speeds 11-3
UPSR
acceptance test 4-23
add a node 13-13
edit UPSR circuit path selectors 8-10
install fiber 1-43
perform a span protection switching test 4-25
provision 4-22
provision path selectors 5-25
remove a node 13-15
subtend a BLSR 4-27
upgrade optical speeds (automatically) 11-3
upgrade optical speeds (spans) 11-8
upgrade to a BLSR 12-6
verify timing after dropping a node 13-12
users
change password or security settings 10-19, 10-20
delete 10-22
user setup 3-3

V

views
overview A-1
change from one view to another A-1
network view actions A-6
shortcuts A-1
virtual link table (OSPF) 3-11
VLAN
provision E Series Ethernet ports 5-65
provision ports for VLAN 5-65
verify VLAN availability 5-63
voltmeter 1-19, 1-49
VT *see* circuits
VT tunnel
automatically-routed 5-28
description 5-2
manually-routed 5-30

W

Windows 2000 2-12, 2-14, 2-16

Windows 95/98 2-11, 2-13, 2-15

Windows NT 2-12, 2-14, 2-16

Windows XP 2-12, 2-14, 2-17

WINS configuration 2-11, 2-13, 2-15, 2-19

wire

- install alarm cables 1-29
- install TL1 craft interface wires 1-32

working card GL-24

WTR (condition) 14-8

X

XTC card

- clear the database for disaster recovery 14-10
- craft interface B-2
- CTC access B-2
- database backup 14-6, 14-15
- modem interface B-2
- reset 14-23
- restore database 14-8
- RJ-45 (LAN) port 2-9, 2-21, 2-22
- soft reset 14-23
- switch test 4-7
- upgrade 11-1