



Cisco ONS 15540 ESPx Configuration Guide

Cisco IOS Release 12.2SV
February 2006

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

Text Part Number: OL-9543-01



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

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

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

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

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

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

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

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

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

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

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.



Preface xvii

Document Objectives	xvii
Audience	xvii
New and Changed Information	xviii
New and Changed Information for Cisco IOS Release 12.2(29)SV	xviii
New and Changed Information for Cisco IOS Release 12.2(24)SV	xviii
New and Changed Information for Cisco IOS Release 12.2(23)SV	xix
New and Changed Information for Cisco IOS Release 12.2(18)SV2	xix
New and Changed Information for Cisco IOS Release 12.2(18)SV	xix
Document Organization	xix
Related Documentation	xx
Document Conventions	xxi
Where to Find Safety and Warning Information	xxii
Obtaining Documentation	xxii
Cisco.com	xxii
Product Documentation DVD	xxii
Cisco Optical Networking Product Documentation CD-ROM	xxiii
Ordering Documentation	xxiii
Documentation Feedback	xxiii
Cisco Product Security Overview	xxiii
Reporting Security Problems in Cisco Products	xxiv
Obtaining Technical Assistance	xxiv
Cisco Technical Support & Documentation Website	xxv
Submitting a Service Request	xxv
Definitions of Service Request Severity	xxv
Obtaining Additional Publications and Information	xxvi

CHAPTER 1

Product Overview 1-1

Cisco ONS 15540 ESPx Hardware Features	1-1
Chassis Overview	1-1
Component Summary	1-3
Transponder Modules	1-4
SM Transponder Modules	1-4
MM Transponder Modules	1-5

- Type 2 Extended Range Transponder Modules with SFP Optics **1-5**
- 10-GE Transponder Modules **1-8**
- Processor Cards **1-8**
- Optical Power Budget **1-8**
- Standards Compliance **1-8**
- Cisco ONS 15540 ESPx Software Feature Overview **1-8**
 - In-Band Message Channel **1-9**
 - Network Management Systems **1-9**
 - Optical Supervisory Channel **1-9**
 - Online Diagnostics **1-10**
 - Network Topologies **1-10**
 - Multiple Trunk Support **1-10**

CHAPTER 2

Before You Begin 2-1

- About the CLI **2-1**
- About Cisco IOS Command Modes **2-1**
 - Listing Cisco IOS Commands and Syntax **2-3**
- Interface Naming Conventions **2-4**
 - Tengigetheretnephy Interfaces **2-6**
 - Transparent Interfaces **2-6**
 - Wave Interfaces **2-7**
 - Waveethernetphy Interfaces **2-7**
 - Wavepatch Interfaces **2-7**
 - Filter Interfaces **2-8**
 - Wdm Interfaces **2-8**
 - Thru Interfaces **2-8**
 - Wdmrelay Interfaces **2-8**
 - Wdmsplit Interfaces **2-8**
 - OSC Interfaces **2-9**
 - Ethernetdcc Interfaces **2-9**
 - NME Interfaces **2-9**
 - Auxiliary Port Interfaces **2-10**
- Configuration Overview **2-10**

CHAPTER 3

Initial Configuration 3-1

- About the Processor Card **3-1**
- Starting Up the Cisco ONS 15540 ESPx **3-2**
- Using the Console Ports, NME Ports, and Auxiliary Ports **3-2**
 - Modem Support **3-2**

About Passwords	3-3
Enable Password	3-3
Enable Secret Password	3-3
Configuring IP Access on the NME Interface	3-3
Displaying the NME Interface Configuration	3-5
Displaying the Operating Configurations	3-6
Configuring the Host Name	3-6
About NTP	3-6
Configuring NTP	3-7
Displaying the NTP Configuration	3-8
Configuring Security Features	3-8
Configuring AAA	3-8
Configuring Authentication	3-8
Configuring Authorization	3-9
Configuring Accounting	3-9
Configuring Kerberos	3-9
Configuring RADIUS	3-9
Configuring TACACS+	3-10
Configuring Secure Shell	3-11
Displaying and Disconnecting SSH	3-12
Testing the System Management Functions	3-12
Displaying Active Processes	3-13
Displaying Protocols	3-13
Displaying Stacks	3-13
Displaying Environment	3-14
Checking Basic Connectivity	3-14
Configuring Traffic Filters and Firewalls	3-14
Configuring Passwords and Privileges	3-14
About Processor Card Redundancy	3-15
Redundant Operation Requirements	3-17
Conditions Causing a Switchover from the Active Processor Card	3-17
Configuring Processor Card Redundancy	3-18
Forcing a Switchover from Privileged EXEC Mode	3-18
Forcing a Switchover from ROM Monitor Mode	3-18
Configuring Autoboot	3-20
Displaying the Autoboot Configuration	3-20
Synchronizing the Configurations	3-21
Synchronizing Configurations Manually	3-21
Enabling and Disabling Automatic Synchronization	3-21

- Configuring Maintenance Mode **3-22**
- Displaying the Processor Card Redundancy Configuration and Status **3-23**
- Reloading the Processor Cards **3-25**
- Configuring Privileged EXEC Mode Access on the Standby Processor Card **3-25**
 - Displaying the Standby Processor Card Privileged EXEC Mode Status **3-26**
- About Preserving Counters on a Processor Card Switchover **3-27**
- Configuring Counter Preservation **3-27**
 - Displaying the Counter Preservation Configuration **3-28**
- About the Software Configuration Register **3-30**
 - Software Configuration Register Settings **3-30**
 - Boot Field Values **3-32**
 - Default System Boot Behavior **3-32**
 - Boot Command **3-33**
- Changing the Software Configuration Register **3-33**
 - Verify the Configuration Register Value **3-34**
- About Fan Failure Shutdown **3-34**
- Configuring Fan Failure Shutdown **3-35**
 - Displaying the Fan Tray Failure Shutdown Configuration **3-35**
- About Critical Temperature Shutdown **3-36**
- Configuring Critical Temperature Shutdown **3-37**
 - Displaying the Threshold Temperatures **3-37**

CHAPTER 4

Configuring 2.5-Gbps Transponder Module Interfaces and Patch Connections 4-1

- Configuring Protocol Encapsulation or Clock Rate **4-2**
 - Displaying Protocol Encapsulation or Clock Rate Configuration **4-6**
- About Protocol Monitoring **4-6**
- Configuring Protocol Monitoring **4-8**
 - Displaying Protocol Monitoring Configuration **4-8**
- About Alarm Thresholds **4-9**
- Configuring Alarm Thresholds **4-9**
 - Displaying Alarm Threshold Configuration **4-12**
- About Laser Shutdown **4-13**
 - About Forward Laser Control **4-13**
 - About Open Fibre Control **4-14**
 - About Laser Safety Control **4-15**
- Configuring Laser Shutdown **4-16**
 - Configuring Forward Laser Control **4-16**
 - Displaying Forward Laser Control Configuration **4-17**

Configuring Laser Safety Control	4-17
Displaying Laser Safety Control Configuration	4-18
Configuring Transponder Channel Frequency	4-18
Displaying Transponder Channel Frequency	4-19
Configuring Optical Power Thresholds	4-19
Displaying Optical Power Threshold Configuration	4-20
About Patch Connections	4-21
Configuring Patch Connections	4-21
Displaying Patch Connections	4-23
About Cross Connections	4-24
Displaying Cross Connections	4-25
About Performance History Counters	4-25
Displaying Performance History Counters	4-26

CHAPTER 5**Configuring 10-GE Transponder Module Interfaces and Patch Connections 5-1**

Enabling Tengigethernetphy Interfaces	5-2
Displaying Tengigethernetphy Interface Information	5-2
Enabling the In-Band Message Channel on Tengigethernetphy Interfaces	5-3
Displaying the In-Band Message Channel Configuration	5-4
Enabling Waveethernetphy Interfaces and Turning on ITU Lasers	5-4
Displaying Waveethernetphy Interface Information	5-5
Configuring Loopbacks	5-5
Displaying Loopback Configuration	5-6
About Alarm Thresholds	5-7
Configuring Alarm Thresholds	5-7
Displaying Alarm Threshold Configuration	5-10
Configuring Forward Laser Control	5-11
Displaying Forward Laser Control Configuration	5-12
Configuring Patch Connections	5-12
Displaying Patch Connections	5-13
Configuring Optical Power Thresholds	5-14
Displaying Optical Power Threshold Configuration	5-14
Turning Lasers On and Off	5-15
Displaying Laser Status	5-16
About Cross Connections	5-16
Displaying Cross Connections	5-17
About Performance History Counters	5-17

Displaying Performance History Counters 5-18

CHAPTER 6

Configuring PSM Interfaces 6-1

- About the PSM 6-1
- Enabling Wdmsplit Interfaces 6-2
 - Displaying Wdmsplit Interface Information 6-2
- Configuring Trunk Fiber Based Protection 6-3
 - Displaying Trunk Fiber Protection Configuration 6-4
- About Switchovers and Optical Power Thresholds 6-4
 - Unamplified Topologies 6-5
 - Post-Amplified Topologies 6-5
 - Post-Amplified and Preamplified Topologies 6-6
- Configuring Optical Power Thresholds 6-8
 - Displaying Optical Power Threshold Configuration 6-9
- Configuring Patch Connections 6-10
 - Displaying Patch Connections 6-10
- Configuring Wdmsplit Interfaces in the Network Topology 6-11
 - Displaying Topology Information for Wdmsplit Interfaces 6-12

CHAPTER 7

Configuring APS 7-1

- About APS 7-1
- About Splitter Protection 7-2
 - Considerations for Using Splitter Protection 7-3
- Configuring Splitter Protection 7-3
 - Displaying the Splitter Protection Configuration 7-5
- About Line Card Protection 7-6
- About Client Based Line Card Protection 7-6
- About Y-Cable Line Card Protection 7-7
 - Considerations for Using Y-Cable Based Line Card Protection 7-8
- Configuring Y-Cable Based Line Card Protection 7-8
 - Displaying the Y-Cable Protection Configuration 7-10
- Configuring Splitter Protected Line Card Motherboards for Line Card Protection 7-11
- About Trunk Fiber Based Protection 7-12
 - Considerations for Using Trunk Fiber Based Protection 7-13
- Configuring Trunk Fiber Based Protection 7-14
 - Displaying Trunk Fiber Protection Configuration 7-14
- Configuring APS Group Attributes 7-15

Configuring Revertive Switching	7-15
Displaying the Revertive Switching Configuration	7-16
About Path Switching	7-17
Configuring Path Switching	7-19
Changing the Path Switching Direction for Y-Cable Protection	7-21
Displaying the Path Switching Configuration	7-23
Configuring the Switchover-Enable Timer	7-24
Displaying the Switchover-Enable Timer Configuration	7-25
Configuring the Wait-to-Restore Timer	7-25
Displaying the Wait-to-Restore Timer Configuration	7-26
Configuring the Search-For-Up Timer	7-27
Displaying the Search-For-Up Timer Configuration	7-28
Configuring the Message Timers	7-28
Displaying the Message Timer Configuration	7-29
Switchovers and Lockouts	7-30
Requesting a Switchover or Lockout	7-31
Displaying Switchover and Lockout Request Status	7-31
Clearing Switchovers and Lockouts	7-32
Displaying Switchover and Lockout Clear Status	7-32

CHAPTER 8**Configuring Dual Shelf Nodes 8-1**

About Dual Shelf Nodes	8-1
Configuring Line Card Protected Dual Shelf Nodes	8-1
Configuring and Cabling the Shelves	8-2
Add/Drop Mux/Demux Modules for 24 Channels	8-2
Configuring Connections Between Shelves	8-5
Configuring APS	8-5

CHAPTER 9**Configuring Point-to-Point Topologies 9-1**

About Point-to-Point Topologies	9-1
Multiple Trunk Support	9-3
Configuring a Point-to-Point Topology with Splitter Protection	9-3
Patch Connections	9-4
Transparent Interfaces	9-5
APS	9-9
Configuring a Point-to-Point Topology with Line Card Protection	9-9
Node 1	9-11
Patch Connections	9-11
Transparent Interfaces	9-12

APS 9-15

Configuring an Unprotected Point-to-Point Topology 9-17

 Patch Connections 9-19

 Transparent Interfaces 9-21

CHAPTER 10

Configuring Ring Topologies 10-1

About Ring Topologies 10-1

 Hubbed Ring Topologies 10-1

 Meshed Ring Topologies 10-2

 Multiple Trunk Support 10-3

Configuring a Hubbed Ring with Splitter Protection and OSC 10-3

 Node 1 10-4

 Patch Connections 10-5

 Transparent Interfaces 10-6

 OSC Interfaces 10-8

 APS 10-8

 Node 2 10-10

 Patch Connections 10-11

 Transparent Interfaces in Slot 2 10-12

 OSC Interfaces 10-12

 APS 10-12

 Node 3 10-13

 Patch Connections 10-14

 Transparent Interfaces in Slot 4 10-14

 OSC Interfaces 10-15

 APS 10-15

 Node 4 10-16

 Patch Connections 10-17

 Transparent Interfaces in Slot 8 10-18

 OSC Interfaces 10-18

 APS 10-18

 Node 5 10-19

 Patch Connections 10-20

 Transparent Interfaces in Slot 11 10-20

 OSC Interfaces 10-21

 APS 10-21

Configuring a Hubbed Ring with Line Card Protection and OSC 10-22

 Node 1 10-22

 Patch Connections 10-23

Transparent Interfaces	10-24
OSC Interfaces	10-27
APS	10-28
Node 2	10-30
Patch Connections	10-31
Transparent Interfaces in Slot 2	10-32
Transparent Interfaces in Slot 4	10-32
OSC Interfaces	10-32
APS	10-33
Node 3	10-34
Patch Connections	10-35
Transparent Interfaces in Slot 3	10-36
Transparent Interfaces in Slot 5	10-36
OSC Interfaces	10-36
APS	10-37
Node 4	10-38
Patch Connections	10-39
Transparent Interfaces in Slot 8	10-40
Transparent Interfaces in Slot 10	10-40
OSC Interfaces	10-40
APS	10-41
Node 5	10-42
Patch Connections	10-43
Transparent Interfaces in Slot 9	10-44
Transparent Interfaces in Slot 11	10-44
OSC Interfaces	10-44
APS	10-45
Configuring a Meshed Ring with Splitter Protection and OSC	10-46
Node 1	10-47
Patch Connections	10-48
Transparent Interfaces in Slot 2	10-49
Transparent Interfaces in Slot 5	10-49
Transparent Interfaces in Slot 8	10-50
OSC Interfaces	10-50
APS	10-50
Node 2	10-52
Patch Connections	10-53
Transparent Interfaces in Slot 2	10-54
OSC Interfaces	10-54
APS	10-54

Node 3	10-55	
Patch Connections	10-56	
Transparent Interfaces in Slot 5	10-57	
Transparent Interfaces in Slot 11	10-57	
OSC Interfaces	10-58	
APS	10-58	
Node 4	10-59	
Patch Connections	10-60	
Transparent Interfaces in Slot 8	10-61	
Transparent Interfaces in Slot 11	10-61	
OSC Interfaces	10-62	
APS	10-62	
Configuring a Splitter Protected Meshed Ring with Unprotected Channels and OSC		10-63
Node 1	10-63	
Node 2	10-64	
Patch Connections	10-65	
Transparent Interfaces in Slot 2	10-66	
Transparent Interfaces in Slot 4	10-66	
OSC Interfaces	10-67	
APS	10-67	
Node 3	10-67	
Patch Connections	10-69	
Transparent Interfaces in Slot 5	10-70	
Transparent Interfaces in Slot 8	10-70	
Transparent Interfaces in Slot 11	10-71	
OSC Interfaces	10-71	
APS	10-71	
Node 4	10-72	
Configuring a Meshed Ring with Line Card Protection and OSC		10-72
Node 1	10-73	
Patch Connections	10-74	
Transparent Interfaces in Slot 2	10-75	
Transparent Interfaces in Slot 3	10-75	
Transparent Interfaces in Slot 4	10-76	
Transparent Interfaces in Slot 5	10-76	
Transparent Interfaces in Slot 8	10-77	
Transparent Interfaces in Slot 10	10-77	
OSC Interfaces	10-78	
APS	10-78	
Node 2	10-80	

Patch Connections	10-81
Transparent Interfaces in Slot 2	10-82
Transparent Interfaces in Slot 4	10-82
OSC Interfaces	10-82
APS	10-83
Node 3	10-84
Patch Connections	10-85
Transparent Interfaces in Slot 3	10-86
Transparent Interfaces in Slot 5	10-86
Transparent Interfaces in Slot 9	10-87
Transparent Interfaces in Slot 11	10-87
OSC Interfaces	10-88
APS	10-88
Node 4	10-89
Patch Connections	10-90
Transparent Interfaces in Slot 8	10-91
Transparent Interfaces in Slot 9	10-91
Transparent Interfaces in Slot 10	10-92
Transparent Interfaces in Slot 11	10-92
OSC Interfaces	10-93
APS	10-93
Configuring a Line Card Protected Meshed Ring with Unprotected Channels and OSC	10-94
Node 1	10-94
Node 2	10-95
Patch Connections	10-96
Transparent Interfaces in Slot 2	10-97
Transparent Interfaces in Slot 4	10-97
Transparent Interfaces in Slot 8	10-98
OSC Interfaces	10-98
APS	10-98
Node 3	10-99
Patch Connections	10-100
Transparent Interfaces in Slot 3	10-101
Transparent Interfaces in Slot 5	10-101
Transparent Interfaces in Slot 8	10-102
Transparent Interfaces in Slot 9	10-102
Transparent Interfaces in Slot 11	10-103
OSC Interfaces	10-103
APS	10-103
Node 4	10-104

CHAPTER 11

Monitoring Your Network Topology 11-1

- About the OSC **11-1**
 - Hardware Guidelines for Using OSC **11-2**
- Configuring CDP **11-3**
 - Configuring Global CDP **11-3**
 - Displaying the Global CDP Configuration **11-4**
 - Displaying Global CDP Information **11-4**
 - Clearing Global CDP Information **11-5**
 - Configuring CDP Topology Discovery on Wdm and Tengigethernetphy Interfaces **11-5**
 - Displaying CDP Information **11-6**
- Configuring OSCP **11-6**
 - Configuring the Hello Interval Timer **11-7**
 - Configuring the Hello Hold-Down Timer **11-7**
 - Configuring the Inactivity Factor **11-7**
 - Displaying the OSCP Configuration **11-8**
 - Displaying OSCP Neighbors **11-8**
- Configuring IP on the OSC **11-9**
 - Verifying Connectivity Over the OSC **11-11**
- Configuring IP on Ethernetdcc Interfaces for the In-Band Message Channel **11-11**
 - Displaying the Ethernetdcc Interface Configuration **11-14**
 - Verifying Connectivity over the In-Band Message Channel **11-14**
- Configuring SNMP **11-14**
 - Enabling MIB Notifications **11-15**
 - Alarm Threshold MIB **11-15**
 - APS MIB **11-16**
 - OSCP MIB **11-16**
 - Patch MIB **11-16**
 - Physical Topology MIB **11-17**
 - Redundancy Facility MIB **11-17**
- Monitoring Without the OSC or In-Band Message Channel **11-18**
 - Setting Up Connections to Individual Nodes **11-18**
 - Manually Configuring the Network Topology **11-18**
 - Displaying the Network Topology **11-19**
- Configuring Interfaces in the Network Topology **11-20**
 - Displaying Topology Information **11-21**
- About Embedded CiscoView **11-21**
- Installing and Configuring Embedded CiscoView **11-21**
 - Accessing Embedded CiscoView **11-24**

Displaying Embedded CiscoView Information 11-24

INDEX



FIGURES

<i>Figure 1-1</i>	Cisco ONS 15540 ESPx Shelf Layout	1-2
<i>Figure 2-1</i>	Cisco ONS 15540 ESPx Interface Model with Splitter Protection	2-5
<i>Figure 2-2</i>	Cisco ONS 15540 ESPx Interface Model with Line Card Protection	2-6
<i>Figure 3-1</i>	Processor Card State Transition Diagram	3-16
<i>Figure 4-1</i>	Forward Laser Control Overview	4-13
<i>Figure 4-2</i>	OFC Overview	4-14
<i>Figure 4-3</i>	Laser Safety Control Overview	4-15
<i>Figure 4-4</i>	Example Splitter Protected Shelf Configuration	4-22
<i>Figure 4-5</i>	Optical Cross Connection Example on the Cisco ONS 15540 ESPx	4-24
<i>Figure 6-1</i>	Optical Patch Connection Example Between a PSM and a Mux/Demux Module	6-2
<i>Figure 6-2</i>	Point-to-Point Topology Without Amplification	6-5
<i>Figure 6-3</i>	Point-to-Point Topology with Post-Amplification	6-6
<i>Figure 6-4</i>	Point-to-point Topology with Post-Amplification and Pre-Amplification	6-7
<i>Figure 6-5</i>	Failure Scenario with Noise from Two EDFAs	6-8
<i>Figure 7-1</i>	Splitter Protection Scheme with 2.5-Gbps Transponder Module	7-2
<i>Figure 7-2</i>	Line Card Protection Scheme with 2.5-Gbps Transponder Module	7-7
<i>Figure 7-3</i>	Trunk Fiber Based Protection Scheme	7-13
<i>Figure 7-4</i>	Active and Standby Path Configuration Example	7-17
<i>Figure 7-5</i>	Unidirectional Path Switching Example	7-18
<i>Figure 7-6</i>	Bidirectional Path Switching Overview	7-18
<i>Figure 7-7</i>	Bidirectional Path Switching Example with Splitter Protection	7-20
<i>Figure 7-8</i>	Bidirectional Path Switching Example with Y-Cable Protection	7-20
<i>Figure 8-1</i>	Shelf 1 Configuration for 24 Channels with Add/Drop Mux/Demux Modules and Line Card Protection	8-2
<i>Figure 8-2</i>	Shelf 2 Configuration for 24 Channels with Add/Drop Mux/Demux Modules and Line Card Protection	8-3
<i>Figure 8-3</i>	Add/Drop Mux/Demux Module Cabling with Two Shelves with 24 Channels and Line Card Protection	8-4
<i>Figure 9-1</i>	Protected Point-to-Point Topology Example	9-2
<i>Figure 9-2</i>	Unprotected Point-to-Point Topology Example	9-2
<i>Figure 9-3</i>	Shelf Configuration for Splitter Protected 32-Channel Point-to-Point Topology	9-3
<i>Figure 9-4</i>	Terminal Mux/Demux Module Cabling with OSC for Splitter Protected 32-Channel Point-to-Point Topology	9-4
<i>Figure 9-5</i>	Shelf Configuration for Line Card Protected 16-Channel Point-to-Point Topology	9-10
<i>Figure 9-6</i>	Terminal Mux/Demux Module Cabling with OSC for Line Card Protected 16-Channel Point-to-Point	

	Topology	9-11
<i>Figure 9-7</i>	Shelf Configuration for Unprotected 32-Channel Point-to-Point Topology	9-18
<i>Figure 9-8</i>	Terminal Mux/Demux Module Cabling with OSC for Unprotected 32-Channel Point-to-Point Topology	9-19
<i>Figure 10-1</i>	Hubbed Ring Topology Example	10-2
<i>Figure 10-2</i>	Meshed Ring Topology Example	10-3
<i>Figure 10-3</i>	Hubbed Ring Channel Plan	10-4
<i>Figure 10-4</i>	Shelf Configuration for 16-Channel Hub Node in Splitter Protected Hubbed Ring	10-4
<i>Figure 10-5</i>	Terminal Mux/Demux Module Cabling with OSC for 16-Channel Hub Node in Splitter Protected Hubbed Ring	10-5
<i>Figure 10-6</i>	Shelf Configuration for Node 2 in Splitter Protected Hubbed Ring	10-10
<i>Figure 10-7</i>	Add/Drop Mux/Demux Module Cabling with OSC for Node 2 in Splitter Protected Hubbed Ring	10-11
<i>Figure 10-8</i>	Shelf Configuration for Node 3 in Splitter Protected Hubbed Ring	10-13
<i>Figure 10-9</i>	Add/Drop Mux/Demux Module Cabling with OSC for Node 3 in Splitter Protected Hubbed Ring	10-14
<i>Figure 10-10</i>	Shelf Configuration for Node 4 in Splitter Protected Hubbed Ring	10-16
<i>Figure 10-11</i>	Add/Drop Mux/Demux Module Cabling with OSC for Node 4 in Splitter Protected Hubbed Ring	10-17
<i>Figure 10-12</i>	Shelf Configuration for Node 5 in Splitter Protected Hubbed Ring	10-19
<i>Figure 10-13</i>	Add/Drop Mux/Demux Module Cabling with OSC for Node 5 in Splitter Protected Hubbed Ring	10-20
<i>Figure 10-14</i>	Shelf Configuration for Hub Node in Line Card Protected Hubbed Ring	10-22
<i>Figure 10-15</i>	Terminal Mux/Demux Module Cabling with OSC for Hub Node in Line Card Protected Hubbed Ring	10-23
<i>Figure 10-16</i>	Shelf Configuration for Node 2 in Line Card Protected Hubbed Ring	10-30
<i>Figure 10-17</i>	Add/Drop Mux/Demux Module Cabling with OSC for Node 2 in Line Card Protected Hubbed Ring	10-31
<i>Figure 10-18</i>	Shelf Configuration for Node 3 in Line Card Protected Hubbed Ring	10-34
<i>Figure 10-19</i>	Add/Drop Mux/Demux Module Cabling with OSC for Node 3 in Line Card Protected Hubbed Ring	10-35
<i>Figure 10-20</i>	Module Installation Configuration for Node 4	10-38
<i>Figure 10-21</i>	Add/Drop Mux/Demux Module Cabling with OSC for Node 4 in Line Card Protected Hubbed Ring	10-39
<i>Figure 10-22</i>	Shelf Configuration for Node 5 in Line Card Protected Hubbed Ring	10-42
<i>Figure 10-23</i>	Add/Drop Mux/Demux Module Cabling with OSC for Node 5 in Line Card Protected Hubbed Ring	10-43
<i>Figure 10-24</i>	Channel Plan for Meshed Ring	10-46
<i>Figure 10-25</i>	Shelf Configuration for Node 1 in Splitter Protected Meshed Ring	10-47
<i>Figure 10-26</i>	Add/Drop Mux/Demux Module Cabling with OSC for Node 1 in Splitter Protected Meshed Ring	10-48
<i>Figure 10-27</i>	Shelf Configuration for Node 2 in Splitter Protected Meshed Ring	10-52
<i>Figure 10-28</i>	Add/Drop Mux/Demux Module Cabling with OSC for Node 2 in Splitter Protected Meshed Ring	10-53
<i>Figure 10-29</i>	Shelf Configuration for Node 3 in Splitter Protected Meshed Ring	10-55
<i>Figure 10-30</i>	Add/Drop Mux/Demux Module Cabling with OSC for Node 3 in Splitter Protected Meshed Ring	10-56
<i>Figure 10-31</i>	Module Installation Configuration for Node 4	10-59
<i>Figure 10-32</i>	Add/Drop Mux/Demux Module Cabling with OSC for Node 4 in Splitter Protected Meshed Ring	10-60

<i>Figure 10-33</i>	Overview of Meshed Ring Topology with Splitter Protection	10-63
<i>Figure 10-34</i>	Shelf Configuration for Node 2 in Splitter Protected Meshed Ring with Unprotected Channels	10-64
<i>Figure 10-35</i>	Add/Drop Mux/Demux Module Cabling for Node 2 in Splitter Protected Meshed Ring with Unprotected Channels	10-65
<i>Figure 10-36</i>	Shelf Configuration for Node 3 in Splitter Protected Meshed Ring with Unprotected Channels	10-68
<i>Figure 10-37</i>	Add/Drop Mux/Demux Module Cabling for Node 3 in Splitter Protected Meshed Ring with Unprotected Channels	10-69
<i>Figure 10-38</i>	Shelf Configuration for Node 1 in Line Card Protected Meshed Ring	10-73
<i>Figure 10-39</i>	Add/Drop Mux/Demux Module Cabling with OSC for Node 1 in Line Card Protected Meshed Ring	10-74
<i>Figure 10-40</i>	Shelf Configuration for Node 2 in Line Card Protected Meshed Ring	10-80
<i>Figure 10-41</i>	Add/Drop Mux/Demux Module Cabling with OSC for Node 2 in Line Card Protected Meshed Ring	10-81
<i>Figure 10-42</i>	Shelf Configuration for Node 3 in Line Card Protected Meshed Ring	10-84
<i>Figure 10-43</i>	Add/Drop Mux/Demux Module Cabling with OSC for Node 3 in Line Card Protected Meshed Ring	10-85
<i>Figure 10-44</i>	Shelf Configuration for Node 4 in Line Card Protected Meshed Ring	10-89
<i>Figure 10-45</i>	Add/Drop Mux/Demux Module Cabling with OSC for Node 4 in Line Card Protected Meshed Ring	10-90
<i>Figure 10-46</i>	Shelf Configuration for Node 2 in Line Card Protected Meshed Ring with Unprotected Channels	10-95
<i>Figure 10-47</i>	Add/Drop Mux/Demux Module Cabling for Node 2 in Line Card Protected Meshed Ring with Unprotected Channels	10-96
<i>Figure 10-48</i>	Shelf Configuration for Node 3 in Line Card Protected Meshed Ring with Unprotected Channels	10-99
<i>Figure 10-49</i>	Add/Drop Mux/Demux Module Cabling for Node 3 in Line Card Protected Meshed Ring with Unprotected Channels	10-100
<i>Figure 11-1</i>	OSC Signal Path in a Ring Configuration	11-2
<i>Figure 11-2</i>	Ring Topology Example	11-19



TABLES

Table 1-1	Fixed Rate SFP Optics Features	1-5
Table 1-2	Variable Rate SFP Optics Features	1-6
Table 2-1	Frequently Used IOS Command Modes	2-2
Table 3-1	Processor Card Hardware States	3-15
Table 3-2	Processor Card Software States	3-16
Table 3-3	Synchronization Events for Configuration Files	3-22
Table 3-4	Counters Preserved Over a Processor Card Switchover	3-27
Table 3-5	Software Configuration Register Bits	3-30
Table 3-6	Register Settings for Broadcast Address	3-31
Table 3-7	Settings for Console Terminal Transmission Rate	3-31
Table 3-8	Configuration Register Boot Field Values	3-32
Table 4-1	Supported Clock Rates for Well-Known Protocols	4-4
Table 4-2	Threshold Error Rates for Monitored Protocols in Errors Per Second	4-10
Table 4-3	Thresholds for Monitored Protocols (Errors Per Second)	4-11
Table 4-4	Patch Connection Types	4-21
Table 5-1	Threshold Error Rates for Monitored Protocols in Errors Per Second	5-8
Table 5-2	Thresholds for Monitored Protocols (Errors Per Second)	5-9



Preface

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
- New and Changed Information
- Document Organization
- Related Documentation
- Document Conventions
- Where to Find Safety and Warning Information
- Obtaining Documentation
- Documentation Feedback
- Cisco Product Security Overview
- Obtaining Technical Assistance
- Obtaining Additional Publications and Information

Document Objectives

This guide explains the features and configuration procedures for the Cisco ONS 15540 ESPx system. Use this guide 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.

New and Changed Information

This section describes the changes and additions to this guide for the releases of the Cisco IOS Release 12.2SV major release for the Cisco ONS 15540 ESPx.

New and Changed Information for Cisco IOS Release 12.2(29)SV

The following table lists the changes and additions to this guide for Cisco IOS Release 12.2(29)SV.

Feature	Description	Location
Performance history counter support on Cisco ONS 15540 ESPx transponder module interfaces.	The performance history counters feature is supported on the Cisco ONS 15540 ESPx transponder module interfaces.	“About Performance History Counters” section on page 4-25 “About Performance History Counters” section on page 5-17
SSHv2 support on Cisco ONS 15540 ESPx.	The Cisco ONS 15540 ESPx supports SSHv2 (Secure Shell).	“Configuring Secure Shell” section on page 3-11

New and Changed Information for Cisco IOS Release 12.2(24)SV

The following table lists the changes and additions to this guide for Cisco IOS Release 12.2(24)SV

Feature	Description	Location
SSH support on the Cisco ONS 15540 ESPx.	The Cisco ONS 15540 ESPx supports SSH (Secure Shell).	“Configuring Secure Shell” section on page 3-11
Counter Preservation on the 2.5-Gbps transponder modules.	The 2.5-Gbps transponder modules and 10-GE transponder modules processor cards support counter preservation on processor card switchovers.	“About Preserving Counters on a Processor Card Switchover” section on page 3-27 “Configuring Counter Preservation” section on page 3-27
SNMPv3 support on the Cisco ONS 15540 ESPx.	This Cisco ONS 15540 ESPx supports SNMPv3.	“Configuring SNMP” section on page 11-14
Multiple trunk support	The Cisco ONS 15540 ESPx supports two or more network topologies connected to one shelf.	“Multiple Trunk Support” section on page 1-10 “Multiple Trunk Support” section on page 9-3 “Multiple Trunk Support” section on page 10-3

New and Changed Information for Cisco IOS Release 12.2(23)SV

The following table lists the changes and additions to this guide for Cisco IOS Release 12.2(23)SV

Feature	Description	Location
ISC links peer mode 1-Gbps support on 2.5-Gbps transponder modules.	The 2.5-Gbps transponders modules support ISC links peer mode at 1 Gbps as well as 2 Gbps.	<p>“Transponder Modules” section on page 1-4</p> <p>“Configuring Protocol Encapsulation or Clock Rate” section on page 4-2</p> <p>“About Protocol Monitoring” section on page 4-6</p>

New and Changed Information for Cisco IOS Release 12.2(18)SV2

The following table lists the changes and addition to this guide for Cisco IOS release 12.2(18)SV2.

Feature	Description	Location
Support for patching a PSM to a transponder module.	The PSM now supports patches directly to a transponder module without requiring a mux/demux module.	<p>“Component Summary” section on page 1-3</p> <p>“Configuring Patch Connections” section on page 6-10</p>

New and Changed Information for Cisco IOS Release 12.2(18)SV

The following table lists the changes and addition to this guide for Cisco IOS release 12.2(18)SV.

Feature	Description	Location
Monitoring for 2-Gbps protocols	The 2.5-Gbps transponder module now supports monitoring for 2-Gbps FC and FICON.	“Transponder Modules” section on page 1-4
Change to show redundancy command syntax	The show redundancy command syntax is changed to show redundancy summary .	“Displaying the Processor Card Redundancy Configuration and Status” section on page 3-23

Document Organization

This Cisco ONS 15540 ESPx Configuration Guide is organized into the following chapters:

- Chapter 1, “Product Overview,” provides an overview of the Cisco ONS 15540 ESPx features and functions.
- Chapter 2, “Before You Begin,” provides basic information about the Cisco ONS 15540 ESPx CLI, IOS mode and naming conventions.
- Chapter 3, “Initial Configuration,” describes how to perform the initial configuration of the Cisco ONS 15540 ESPx.
- Chapter 4, “Configuring 2.5-Gbps Transponder Module Interfaces and Patch Connections,” describes how to configure 2.5-Gbps transponder module interfaces and patch connections.

- Chapter 5, “Configuring 10-GE Transponder Module Interfaces and Patch Connections,” describes how to configure 10-GE transponder module interfaces and patch connections.
- Chapter 6, “Configuring PSM Interfaces,” describes how to configure protection switch module interfaces.
- Chapter 7, “Configuring APS,” describes how to configure splitter protection and line card protection with automatic protection switching (APS).
- Chapter 8, “Configuring Dual Shelf Nodes,” describes how to configure a dual shelf node in a network topology.
- Chapter 9, “Configuring Point-to-Point Topologies,” describes how to configure point-to-point topologies.
- Chapter 10, “Configuring Ring Topologies,” describes how to configure ring topologies.
- Chapter 11, “Monitoring Your Network Topology,” describes how to configure and manage your network topology.

Related Documentation

Use this Cisco ONS 15540 ESPx Configuration Guide in conjunction with the following referenced publications:

- *Regulatory Compliance and Safety Information for the Cisco ONS 15500 Series*
Provides the regulatory compliance and safety information for the Cisco ONS 15500 Series.
- *Cisco ONS 15540 ESPx Planning Guide*
Provides detailed information on the Cisco ONS 15540 ESPx architecture and functionality.
- *Cisco ONS 15540 ESPx Hardware Installation Guide*
Provides detailed information about installing the Cisco ONS 15540 ESPx.
- *Cisco ONS 15540 ESPx Optical Transport Turn-Up and Test Guide*
Provides acceptance testing procedures for Cisco ONS 15540 ESPx nodes and networks.
- *Cisco ONS 15540 ESPx Cleaning Procedures for Fiber Optic Connections*
Provides processes and procedures for cleaning the fiber optic connectors and component interfaces of the Cisco ONS 15540 ESPx.
- *Cisco ONS 15540 ESPx Command Reference*
Provides commands to configure and manage the Cisco ONS 15540 ESPx.
- *Cisco ONS 15540 ESPx System Alarms and Error Messages*
Describes the system alarms and error messages for the Cisco ONS 15540 ESPx.
- *Cisco ONS 15540 ESPx Troubleshooting Guide*
Describes how to identify and resolve problems with the Cisco ONS 15540 ESPx.
- *Network Management for the Cisco ONS 15540 ESPx*
Provides information on the network management systems that support the Cisco ONS 15540 ESPx.
- *Cisco ONS 15540 ESPx TL1 Command Reference*
Provides a full TL1 command and autonomous message set including parameters, AIDs, conditions and modifiers for the Cisco ONS 15540 ESPx.

- *MIB Quick Reference for the Cisco ONS 15500 Series*
Describes the Management Information Base (MIB) objects and explains how to access Cisco public MIBs for the Cisco ONS 15500 Series.
- *Cisco ONS 15540 ESPx Software Upgrade Guide*
Describes how to upgrade system images and functional images on the Cisco ONS 15540 ESPx.
- *Introduction to DWDM Technology*
Provides background information on the dense wavelength division multiplexing (DWDM) technology.
- *Cisco IOS Configuration Fundamentals Configuration Guide*
Provides useful information on the CLI (command-line interface) and basic shelf management.

Document Conventions

This publication uses the following conventions:

Convention	Application
boldface	Commands and keywords in body text.
<i>italic</i>	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.



Note

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



Caution

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

**Warning****IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Where to Find Safety and Warning Information

For safety and warning information, refer to the *Cisco Optical Transport Products Safety and Compliance Information* document that accompanied the product. This publication describes the international agency compliance and safety information for the Cisco ONS 15xxx systems. It also includes translations of the safety warnings that appear in the ONS 15xxx system documentation.

Obtaining Documentation

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

Cisco.com

You can access the most current Cisco documentation at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

Cisco Optical Networking Product Documentation CD-ROM

Optical networking-related documentation, including Cisco ONS 15xxx product documentation, is available in a CD-ROM package that ships with your product. The Optical Networking Product Documentation CD-ROM is updated periodically and may be more current than printed documentation.

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation 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.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

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

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

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

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

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

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

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

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—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.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

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

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

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

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

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

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

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

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



Product Overview

The Cisco ONS 15540 ESPx (Extended Services Platform External) are optical transport platforms that employ DWDM (dense wavelength division multiplexing) technology. With the Cisco ONS 15540 ESPx, users can take advantage of the availability of dark fiber to build a common infrastructure that supports data, SAN (storage area network), and TDM (time-division multiplexing) traffic. For more information about DWDM technology and applications, refer to the *Introduction to DWDM Technology* publication and the *Cisco ONS 15540 ESPx Planning Guide*.



Note

To ensure the installed Cisco IOS software supports your hardware and provides the software features you wish to use, see the “New and Changed Information” section on page xviii. Also refer to the “Hardware Supported” section and “Feature Set” section of the latest release notes for the Cisco ONS 15540 ESPx.

This chapter includes the following sections:

- Cisco ONS 15540 ESPx Hardware Features, page 1-1
- Cisco ONS 15540 ESPx Software Feature Overview, page 1-8

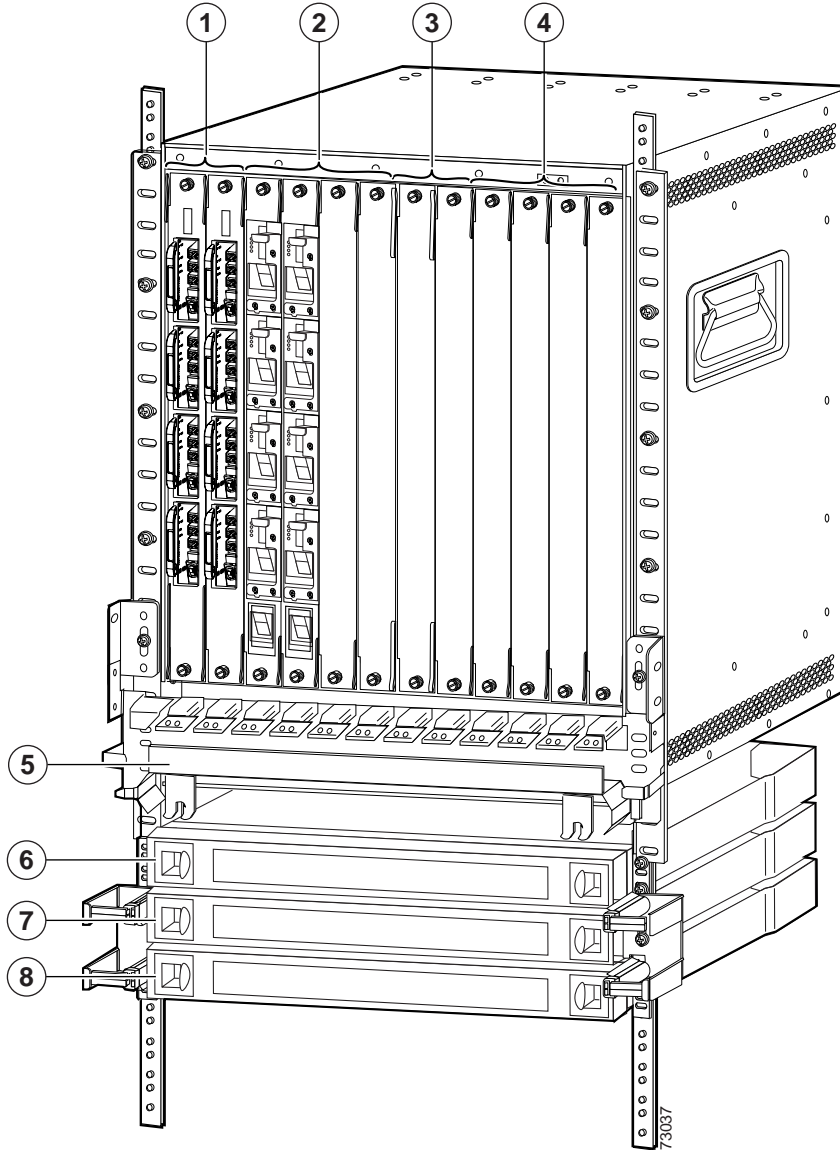
Cisco ONS 15540 ESPx Hardware Features

This section describes the hardware features and components of the Cisco ONS 15540 ESPx.

Chassis Overview

The Cisco ONS 15540 ESPx uses a 12-slot modular vertical chassis. As you face the chassis, the two leftmost slots (slots 0 and 1) hold the optical mux/demux motherboards, which are populated with optical mux/demux modules. Slots 2 through 5 and 8 through 11 hold the line card motherboards, which are populated with transponder modules. Slots 6 and 7 hold the processor cards (see Figure 1-1). Air inlet, fan tray, and cable management are located beneath the modular slots. The system has an electrical backplane for system control.

Figure 1-1 Cisco ONS 15540 ESPx Shelf Layout



1	Slots 0 and 1 hold the mux/demux motherboards	5	Cable management tray
2	Slots 2 to 5 hold the line card motherboards	6	Cable storage drawer
3	Slots 6 and 7 hold the processor cards	7	8-channel cross connect drawer
4	Slots 8 to 11 hold the line card motherboards	8	8-channel cross connect drawer

Component Summary

The Cisco ONS 15540 ESPx supports the following hot-swappable modular hardware components:

- 2.5-Gbps line card motherboards—Up to eight in a system, each of which accepts up to four 2.5-Gbps transponder modules and provides an optical connection on the front panel that carries the channel signals to and from the transponder modules. The Cisco ONS 15540 ESPx supports two types of line card motherboards: splitter protected and unprotected. The splitter protected line card motherboard has two optical connections on the front panel; the unprotected line card motherboard has only one.
- 10-Gbps line card motherboards—Up to eight in a system, each of which accepts up to two 10-GE transponder modules and provides an optical connection on the front panel that carries the signal to and from the mux/demux modules. The Cisco ONS 15540 ESPx supports two types of line card motherboards: splitter protected and unprotected. The splitter protected motherboard has two optical connections on the front panel; the unprotected motherboard has only one.
- Type 1 transponder modules—Up to four per line card motherboard. Each Type 1 transponder module has a single fixed external interface to the client side and an internal interface that connects to the line card motherboards. The transponder modules are hot pluggable, permitting in-service upgrades and replacement. The transponder modules transmit the ITU wavelength, or channel, to the mux/demux modules through the optical connection on the front panel on the line card motherboard. The modules can have either single-mode or multimode client side interfaces.
- Type 2 extended range transponder modules—Up to four per line card motherboard. Each Type 2 extended range transponder module has a single external pluggable interface on the client side and an internal interface that connects to the line card motherboards. The transponder modules are hot pluggable, permitting in-service upgrades and replacement. The transponder modules transmit the ITU wavelength, or channel, to the mux/demux modules through the optical connection on the front panel on the line card motherboard. The small form-factor pluggable optics support various protocols.
- 10-GE transponder modules—Up to two per 10-Gbps line card motherboard. Each 10-GE transponder module has a single external interface to the client side and an internal interface that connects to the 10-Gbps line card motherboard. This interface can connect to the Cisco ONS 15530 or any other native 10-GE interfaces. The 10-GE transponder modules are hot pluggable, permitting in-service upgrades and replacement.
- Optical mux/demux motherboards—Up to two per system, depending on the number of channels supported and the type of protection. The mux/demux motherboard accepts up to four mux/demux modules. There are two types of mux/demux motherboard, with and without OSC support.
- OADM(optical add/drop multiplexing) modules—Up to four per mux/demux motherboard. Each OADM module can multiplex and demultiplex a band of 4 or 8 channels, for a maximum of 32 data channels and the OSC. Channels not filtered by the OADM module are passed on to the next add/drop mux/demux module.
- Optical terminal mux/demux modules—One per mux/demux motherboard. Each terminal mux/demux module can multiplex and demultiplex a band of 32 data channels and the OSC. All of the channels received by the terminal mux/demux modules are terminated, none are passed through.
- Protection switch modules—One per shelf. The PSM provides trunk fiber protection for Cisco ONS 15540 ESPx systems configured in point-to-point topologies. The PSM can connect to either a mux/demux module or a transponder module. The PSM sends the signal to both the west and east directions. It receives both the west and east signals and sends one to either the mux/demux module to be demultiplexed or to the transponder module directly. Both nodes in the network must have the same shelf configuration. When a trunk fiber cut occurs on the active path, the PSM switches the received signal to the standby path.

- Processor cards—Two per system for fault tolerance. The processor cards provide system processing, redundancy arbitration, clocking, and other central functions.
- Cross connect drawers—Up to four per system. The cross connect drawers provides the flexibility to add and drop less than four channels in a band while passing the remaining channels through to another node in the network. Each cross connect drawer supports up to 8 channels.

Transponder Modules

In the transponder module, the client signal is converted into an ITU-compliant wavelength, which is cross-connected to the mux/demux modules. You can populate the line card motherboard subcard slots with as few or as many transponder modules as required (up to 32) to support the desired number of client signals, or data channels.

All client signals are supported in 3R (reshape, retime, retransmit) mode, regardless of protocol encapsulation type.

The Cisco ONS 15540 ESPx supports the following types of single interface transponder modules:

- SM (single-mode) transponder modules
- MM (multimode) transponder modules
- Type 2 extended range transponder modules with SFP optics
- 10-GE transponder modules

SM Transponder Modules

SM transponder modules have fixed, nonpluggable transceivers for the single client interface. SM transponder modules accept SM client signals on the 1310-nm wavelength through an SC connector and support client signal clock rates ranging from 16 Mbps to 2.5 Gbps.

The following protocol encapsulation types are supported in 3R mode plus protocol monitoring:

- ESCON (Enterprise System Connection) (200 Mbps) SM
- Fibre Channel (1 Gbps and 2 Gbps) SM
- FICON (Fiber Connection) (1 Gbps and 2 Gbps) SM
- Gigabit Ethernet (1250 Mbps) SM
- ISC (InterSystem Channel) links compatibility mode SM
- ISC links peer mode (1 Gbps and 2 Gbps) SM
- SDH (Synchronous Digital Hierarchy) STM-1 SM
- SDH STM-4 SM
- SDH STM-16 SM
- SONET OC-3 SM
- SONET OC-12 SM
- SONET OC-48 SM

The following protocol encapsulation types are supported in 3R mode without protocol monitoring:

- Fast Ethernet SM
- FDDI SM

- Sysplex CLO (control link oscillator) MM (8 Mbps)
- Sysplex ETR (external timer reference) MM (8 Mbps)

The SM transponder modules also support the OFC (open fiber control) safety protocol for Fibre Channel, ISC compatibility mode, and FICON.

MM Transponder Modules

MM transponder modules have fixed, nonpluggable transceivers for the single client interface. MM transponder modules accept both SM client signals and MM client signals on the 1310-nm wavelength through an SC connector and support client signal clock rates ranging from 16 Mbps to 622 Mbps.

The following protocol encapsulation types are supported in 3R mode plus protocol monitoring:

- ESCON (200 Mbps) SM and MM
- SDH STM-1 SM and MM
- SDH STM-4 SM and MM
- SONET OC-3 SM and MM
- SONET OC-12 SM and MM

The following protocol encapsulation types are supported in 3R mode without protocol monitoring:

- Fast Ethernet SM
- FDDI SM
- Sysplex CLO (control link oscillator) MM (8 Mbps)
- Sysplex ETR (external timer reference) MM (8 Mbps)

Type 2 Extended Range Transponder Modules with SFP Optics

The Type 2 extended range transponder module accepts two types of SFP optics:

- Fixed rate
- Variable rate

Fixed rate SFP optics modules support specific protocols. Table 1-1 lists the features for the fixed rate SFP optics supported by the Type 2 extended range transponder modules.

Table 1-1 Fixed Rate SFP Optics Features

Part Number	Supported Protocols	Fiber Type	Wavelength	Connector Type
15500-XVRA-01A2	ESCON, SONET OC-3 SR, SDH STM-1	MM 50/125 μ m MM 62.5/125 μ m	1310 nm	MT-RJ
15500-XVRA-02C1	Gigabit Ethernet ¹ , Fibre Channel (1 Gbps) ² , FICON (1 Gbps), ISC-1 (1-Gbps)	MM 50/125 μ m MM 62.5/125 μ m	850 nm	LC
15500-XVRA-02C2	Fibre Channel (1 Gbps and 2 Gbps) ³ , FICON (1 Gbps and 2 Gbps), ISC-3 (1-Gbps and 2-Gbps)	MM 50/125 μ m MM 62.5/125 μ m	850 nm	LC

Table 1-1 Fixed Rate SFP Optics Features (continued)

Part Number	Supported Protocols	Fiber Type	Wavelength	Connector Type
15500-XVRA-03B1	Gigabit Ethernet ⁴ , Fibre Channel (1 Gbps) ⁵ , FICON (1 Gbps), ISC compatibility mode (1 Gbps), ISC peer mode (1 Gbps)	SM 9/125 μ m	1310 nm	LC
15500-XVRA-03B2	Fibre Channel (1 Gbps ⁶ and 2 Gbps ⁷), FICON (1 Gbps and 2 Gbps), ISC compatibility mode (1 Gbps), ISC peer mode (1 Gbps and 2 Gbps)	SM 9/125 μ m	1310 nm	LC
15500-XVRA-06B1	SONET OC-12 SR ⁸ , SDH STM-4	SM 9/125 μ m	1310 nm	LC
15500-XVRA-07B1	SONET OC-48 SR, SDH STM-16	SM 9/125 μ m	1310 nm	LC

1. 1000BASE-SX
2. FC-0-100-M5-SN-S and FC-0-100-M6-SN-S standards
3. FC-0-200-M5-SN-S and FC-0-200-M6-SN-S standards
4. 1000BASE-LX
5. FC-0-100-SM-LC-S standard
6. FC-0-100-SM-LC-S standard
7. FC-0-200-SM-LC-S standard
8. SR = short range

Variable rate SPF optics modules support a range of clock rates. Table 1-2 lists features for the variable rate SFP optics supported by the Type 2 extended range transponder modules.

Table 1-2 Variable Rate SFP Optics Features

Part Number	Clock Rate Range	Protocol Encapsulations Supported	Fiber Type	Wavelength	Connector Type
15500-XVRA-10A1	Low-band 8 Mbps to 200 Mbps	Sysplex (CLO and ETR) ¹ (8 Mbps), Fast Ethernet ² (125 Mbps), SONET OC-3 ³ (155.52 Mbps), SDH STM-1 (622 Mbps), ESCON ⁴ (200 Mbps)	MM 50/125 μ m 62.5/125 μ m	1310 nm	LC
15500-XVRA-10B1	Low-band 8 Mbps to 200 Mbps	Sysplex (CLO and ETR) ¹ (8 Mbps), Fast Ethernet ² (125 Mbps), SONET OC-3 ³ (155.52 Mbps), SDH STM-1 (155.52 Mbps), ESCON ⁴ (200 Mbps)	SM 9/125 μ m	1310 nm	LC
15500-XVRA-11A1	Mid-band 200 Mbps to 622 Mbps	ESCON ⁴ (200 Mbps), SONET OC-12 ³ (622 Mbps), SDH STM-4 (622 Mbps)	MM 50/125 μ m 62.5/125 μ m	1310 nm	LC

Table 1-2 Variable Rate SFP Optics Features (continued)

Part Number	Clock Rate Range	Protocol Encapsulations Supported	Fiber Type	Wavelength	Connector Type
15500-XVRA-11B1	Mid-band 200 Mbps to 1.25 Gbps	ESCON ⁴ (200 Mbps), SONET OC-12 ³ (622 Mbps), SDH STM-4 (622 Mbps), FC ⁴ (1.062 Gbps), FICON (1.062 Gbps), GE ⁴ (LX) (1.250 Gbps) ISC compatibility mode (1.062 Gbps), ISC peer mode (1.062 Gbps)	SM 9/125 μm	1310 nm	LC
15500-XVRA-12B1	High-band 1.062 Gbps to 2.488 Gbps	FC ⁴ (1.062 Gbps and 2.125 Gbps), FICON (1.062 Gbps and 2.125 Gbps), GE ⁴ (LX) (1.250 Mbps), SONET OC-48 (2.488 Gbps), SDH STM-16 (2.488 Gbps), ISC compatibility mode (1.062 Gbps), ISC peer mode (1.062 Gbps and 2.125 Gbps)	SM 9/125 μm	1310 nm	LC

1. Manchester coded
2. 4B/5B coded
3. Scrambler 2²³⁻¹
4. 8B/10B coded

**Note**

The Cisco IOS software only supports Cisco-certified SFP optics on the Type 2 extended range transponder module.

The following protocols can be monitored with the Type 2 extended range transponder modules:

- ESCON (Enterprise Systems Connection)
- Fibre Channel (1 Gbps and 2 Gbps) SM
- FICON (Fiber Connection) (1 Gbps and 2 Gbps) SM
- Gigabit Ethernet (1250 Mbps) SM
- ISC (InterSystem Channel) links compatibility mode SM
- ISC (InterSystem Channel) links peer mode (1-Gbps and 2-Gbps) SM
- SDH (Synchronous Digital Hierarchy) (STM-1, STM-4, STM-16)
- SDH (Synchronous Digital Hierarchy) STM-1 SM
- SONET (OC-3, OC-12, OC-48)

The Type 2 extended range transponder modules also support the OFC (open fiber control) safety protocol for Fibre Channel.

10-GE Transponder Modules

The 10-GE transponder module occupies half the height of the chassis slot and supports the IEEE 802.3ae specification for 10GBASE-LR interfaces. Up to two 10-GE transponder modules occupy a 10-Gbps line card motherboard.

Each 10-GE transponder module supports one client side and one trunk side interface. The client side is a short-reach 1310 nm interface and the trunk side interface is an ITU grid compliant long-reach interface. The transmitter supports a 1260 nm to 1355 nm wavelength range. The 10-GE transponder module is available in 32 versions, one for each of the 32 ITU wavelengths.

Network topologies that use 10-GE transponder modules might require Cisco ONS 15216 Dispersion Compensator Units.

Processor Cards

The Cisco ONS 15540 ESPx includes two processor cards for redundancy, one in active mode and the other in hot-standby mode. Each processor card has a number of subsystems, including a CPU, a clock subsystem, an Ethernet switch for communication between processors and with the LRC (line card redundancy controller) on the mux/demux and line card motherboards, and an SRC (switch card redundancy controller). The active processor controls the system. All motherboards in the system use the system clock and synchronization signals from the active processor. Interfaces on the processor cards permit access by 10/100 Ethernet, console terminal, or modem connections.

Optical Power Budget

On the trunk side, the Cisco ONS 15540 ESPx has an output (laser) power in the range of 6 to 8 dBm and a receive (detector) sensitivity of -32 dBm. For more information on power budget planning, refer to the *Cisco ONS 15540 ESPx Planning Guide*. For power budget specifications for individual components, refer to the *Cisco ONS 15540 ESPx Hardware Installation Guide*.

Standards Compliance

For information on standards compliance for the Cisco ONS 15540 ESPx, refer to the *Regulatory Compliance and Safety Information for the Cisco ONS 15500 Series* publication.

Cisco ONS 15540 ESPx Software Feature Overview

The Cisco ONS 15540 ESPx offers the following software functionality:

- Cisco IOS software on the processor.
- Autoconfiguration at system boot.
- Autodiscovery of network neighbors.
- Online diagnostics.
- SSH (Secure Shell)
- Processor redundancy provided by arbitration of processor status and switchover in case of failure without loss of connections.

- Autosynchronization of startup and running configurations between redundant processor cards.
- Autosynchronization of traffic statistics and performance monitoring counters.
- Support for in-service software upgrades.
- Support for per-channel APS (Automatic Protection Switching) in point-to-point and ring topologies using redundant subsystems that monitor link integrity and signal quality.
- Trunk fiber based DWDM signal protection using APS in point-to-point topologies.
- Support for in-band message channel.
- Unidirectional and bidirectional 1+1 path switching.
- System configuration and management through the CLI (command-line interface), accessible through an Ethernet connection or console terminal.
- Optical power monitoring on the trunk side of the transponder module, digital monitoring on both client and trunk sides of the transponder module, and per-channel transponder module in-service and out-of-service loopback (client and trunk sides).
- Optional out-of-band management of other Cisco ONS 15540 ESPx systems on the network through the OSC (optical supervisory channel).
- Support for network management systems that use SNMP. Its capabilities include configuration management, fault isolation, topology discovery, and path trace.

In-Band Message Channel

The in-band message channel establishes a method for providing OAM&P (operations, administration, management, and provisioning) functions in Ethernet packet-based optical networks without a SONET layer or SDH layer. The in-band message channel terminates with the data channel, not at each node as does the OSC, and provides management on a per wavelength basis.

Network Management Systems

The Cisco ONS 15540 ESPx is supported by the following network management systems:

- CiscoView
- Resource Manager Essentials
- Campus Manager
- CTM (Cisco Transport Manager)

For Embedded CiscoView configuration information, see the “Installing and Configuring Embedded CiscoView” section on page 11-21.

For more information on the network management systems that support the Cisco ONS 15540 ESPx, see the *Network Management for the Cisco ONS 15540 ESPx* publication.

Optical Supervisory Channel

The Cisco ONS 15540 ESPx supports an optional out-of-band management channel for communicating between systems on the network. Using a 33rd wavelength (channel 0), the OSC allows control and management traffic to be carried without a separate Ethernet connection to each Cisco ONS 15540 ESPx

in the network. The OSC always terminates on a neighboring node. By contrast, data channels may or may not be terminated on a given node, depending on whether the channels on the mux/demux modules are treated as either express (pass-through) or add/drop channels.

The OSC carries the following types of information:

- CDP (Cisco Discovery Protocol) packets—Used to discover neighboring devices
- IP packets—Used for SNMP and Telnet sessions between nodes
- OSCP (OSC Protocol) packets—Used to determine whether the OSC link is up using a Hello protocol
- APS protocol packets—Used for controlling signal path switching

**Note**

When the OSC is not present, Cisco ONS 15540 ESPx systems can be managed individually by separate Ethernet connections.

The OSC uses a dedicated laser and detector on a mux/demux motherboard. The OSC is a full duplex channel that can use a single ring for transmit and receive.

For more information on the OSC and managing Cisco ONS 15540 ESPx networks, see Chapter 11, “Monitoring Your Network Topology.”

Online Diagnostics

The Cisco ONS 15540 ESPx provides the following types of online diagnostic tests:

- Background tests checking system component status and access
- OIR (online insertion and removal) tests for motherboards, modules, and standby processors

Network Topologies

The Cisco ONS 15540 ESPx supports the following types of topologies:

- Point-to-point
- Hubbed ring
- Meshed ring

For more information on network topologies, refer to the *Introduction to DWDM Technology* publication and the *Cisco ONS 15540 ESPx Planning Guide*. Also, for information about configuring network topologies, see Chapter 9, “Configuring Point-to-Point Topologies,” and Chapter 10, “Configuring Ring Topologies.”

Multiple Trunk Support

The Cisco ONS 15540 ESPx allows two or more trunks to connect to a single shelf. Both point-to-point topologies and ring topologies are allowed in a multiple trunk configuration. All of the trunks can support optical protection but the OSC will only be available as the APS message channel and network management for one trunk. The other trunk must use either the in-band message channel or an IP connection for the APS message channel and network management.



Before You Begin

This chapter provides basic information about the Cisco ONS 15540 ESPx. This chapter includes the following topics:

- About the CLI, page 2-1
- About Cisco IOS Command Modes, page 2-1
- Interface Naming Conventions, page 2-4
- Configuration Overview, page 2-10

About the CLI

You can configure the Cisco ONS 15540 ESPx from the CLI (command-line interface) that runs on the system console or terminal, or by using remote access.

To use the CLI, your terminal must be connected to the Cisco ONS 15540 ESPx through the console port or one of the TTY lines. By default, the terminal is configured to a basic configuration, which should work for most terminal sessions.

About Cisco IOS Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. To get a list of the commands available in a given mode, type a question mark (?) at the system prompt.

When you start a session on the system, you begin in user mode, also called EXEC mode. Only a limited subset of the commands are available in EXEC mode. To have access to all commands, you must enter privileged EXEC mode. Normally, you must type in a password to access privileged EXEC mode. From privileged mode, you can type in any EXEC command or access global configuration mode. Most of the EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The EXEC commands are not saved across system reboots or across processor switchovers.

You can monitor and control the standby processor with commands entered on the active processor. A subset of EXEC and privileged EXEC commands are available through the standby processor console.



Note

You can easily determine if you are accessing the active or the standby processor: The standby processor has “sby-” prefixed to the command prompt.

The configuration modes allow you to make changes to the running configuration. If you later save the configuration, these commands are stored across system reboots. You must start at global configuration mode. From global configuration mode, you can enter interface configuration mode, subinterface configuration mode, and a variety of submodes.

ROM (read-only memory) monitor mode is a separate mode used when the system cannot boot properly. For example, your system or access server might enter ROM monitor mode if it does not find a valid system image when it is booting, or if its configuration file is corrupted at startup.

Table 2-1 lists and describes the most commonly used modes, how to enter the modes, and the resulting system prompts. The system prompt helps you identify which mode you are in and, therefore, which commands are available to you.

Table 2-1 Frequently Used IOS Command Modes

Mode	Description of Use	How to Access	Prompt
User EXEC	To connect to remote devices, change terminal settings on a temporary basis, perform basic tests, and display system information.	Log in.	Switch>
Privileged EXEC (Enable)	To set operating parameters. The privileged command set includes the commands in user EXEC mode, as well as the configure command. Use this command to access the other command modes.	From the user EXEC mode, enter the enable command and the enable password.	Switch#
Global configuration	To configure features that affect the system as a whole.	From the privileged EXEC mode, enter the configure terminal command.	Switch(config)#
Interface configuration	To enable features for a particular interface. Interface commands enable or modify the operation of a port.	From global configuration mode, enter the interface type location command. For example, enter interface fastethernet 0	Switch(config-if)#
Line configuration	To configure the console port or VTY line from the directly connected console or the virtual terminal used with Telnet.	From global configuration mode, enter the line console 0 command to configure the console port, or the line vty line-number command to configure a VTY line.	Switch(config-line)#
Redundancy configuration	To configure system redundancy.	From global configuration mode, enter the redundancy command.	Switch(config-red)#
APS ¹ configuration	To configure APS redundancy features.	From redundancy configuration mode, enter the associate group command.	Switch(config-aps)#

Table 2-1 Frequently Used IOS Command Modes (continued)

Mode	Description of Use	How to Access	Prompt
Threshold list configuration	To configure alarm threshold list attributes and thresholds.	From the global configuration mode, enter the threshold-list command.	Switch(config-t-list)#
Threshold configuration	To configure alarm threshold attributes.	From threshold list configuration mode, enter the threshold command.	Switch(config-threshold)#

1. Automatic Protection Switching

The Cisco IOS command interpreter, called the EXEC, interprets and executes the commands you enter. You can abbreviate commands and keywords by entering just enough characters to make the command unique from other commands. For example, you can abbreviate the **show** command to **sh** and the **configure terminal** command to **conf t**.

When you type **exit**, the CLI backs out one command mode level. In general, typing **exit** returns you to global configuration mode. To exit configuration mode completely and return to privileged EXEC mode, press **Ctrl-Z** or **end**.

Listing Cisco IOS Commands and Syntax

In any command mode, you can get a list of available commands by entering a question mark (?).

```
Switch> ?
```

To obtain a list of commands that begin with a particular character sequence, type in those characters followed immediately by the question mark (?). Do not include a space. This form of help is called word help, because it lists the words for you.

```
Switch# c?
calendar cd clear clock configure
connect copy
```

To list keywords or arguments, enter a question mark in place of a keyword or argument. Include a space before the question mark. This form of help is called command syntax help, because it reminds you which keywords or arguments are applicable based on the command, keywords, and arguments you have already entered.

```
Switch# configure ?
memory          Configure from NV memory
network         Configure from a TFTP network host
overwrite-network Overwrite NV memory from TFTP network host
terminal        Configure from the terminal
<cr>
```

To redisplay a command you previously entered, press the Up-arrow key. You can continue to press the Up-arrow key to see more previously issued commands.

**Tip**

If you are having trouble entering a command, check the system prompt and enter the question mark (?) for a list of available commands. You might be in the wrong command mode or using incorrect syntax.

You can press **Ctrl-Z** or **end** in any mode to immediately return to privileged EXEC (enable) mode, instead of entering **exit**, which returns you to the previous mode.

Interface Naming Conventions

The Cisco ONS 15540 ESPx has three types of motherboards, the line card motherboard, the 10-GE motherboard, and the mux/demux motherboard. Each line card motherboard can have up to four transponder modules. Each transponder module has two interfaces: an external client side interface and an internal trunk side interface. The client side interface connects to client equipment. The trunk side interface connects to a mux/demux module in a mux/demux motherboard. The interfaces of each mux/demux module connect to a pair of fibers, one for the receive direction and one for the transmit direction. The Cisco ONS 15540 ESPx CLI supports the following interface types:

- Tengietheretnetphy interfaces
- Transparent interfaces
- Wave interfaces
- Waveetheretnetphy interfaces
- Wavepatch interfaces
- Filter interfaces
- Wdm interfaces
- Thru interfaces
- Wdmrelay interfaces
- Wdmsplit interfaces
- OSC (optical supervisory channel) interfaces
- Ethernetdcc interfaces
- NME (network management Ethernet) interfaces
- Auxiliary interface

Figure 2-1 shows the interface relationships on the Cisco ONS 15540 ESPx for splitter protected line card motherboards with transparent transponder modules and mux/demux motherboards with mux/demux modules and the OSC.

Figure 2-1 Cisco ONS 15540 ESPx Interface Model with Splitter Protection

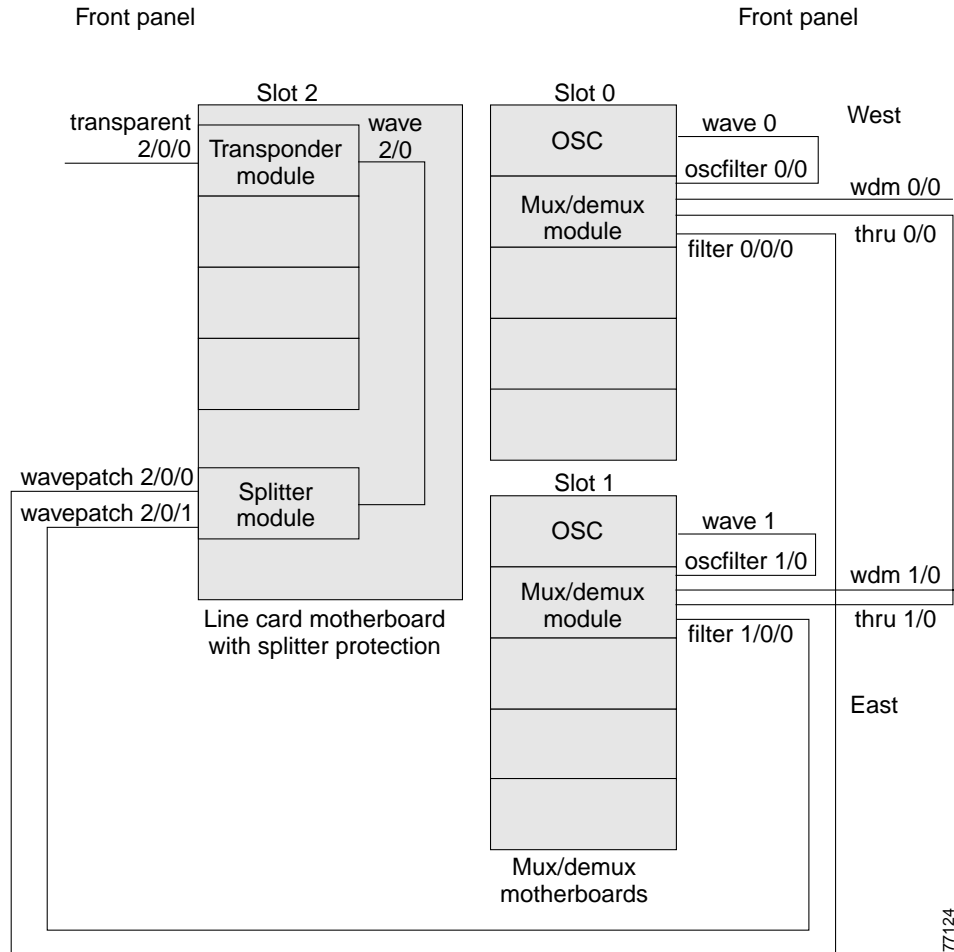
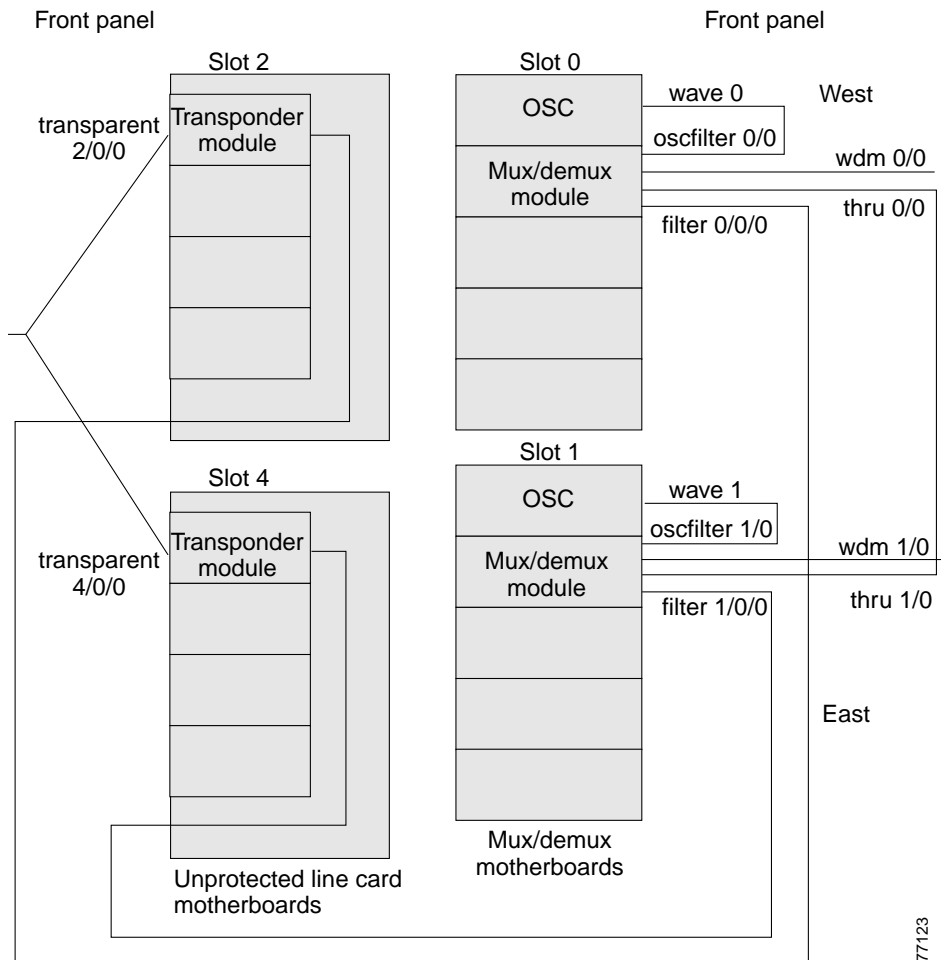


Figure 2-2 shows the interface relationship on the Cisco ONS 15540 ESPx for unprotected line card motherboards with transparent transponder modules and mux/demux motherboards with mux/demux modules and the OSC.

Figure 2-2 Cisco ONS 15540 ESPx Interface Model with Line Card Protection



Tengigethernetphy Interfaces

The tengigethernetphy interfaces are the client side interfaces of the 10-GE transponder modules. This uncolored interface carries 10-GE physical layer signals. It does not terminate layer 2 or layer 3 protocol operations.

The naming convention for the tengigethernetphy interfaces on the 10-GE transponder module is as follows:

tengigethernetphy slot/subcard/port

Transparent Interfaces

The transparent interfaces are the client side interfaces on the transponder modules. The interface does not terminate the protocol, hence the term *transparent*. Also, transparent applies to transparency with regard to networking protocols. The transparent interface connects to the wave interface on the ITU side of the transponder module (see Figure 2-1).

The naming convention for the client side interfaces on the transponder module is as follows:

transparent *slot/subcard/port*

Because the client side of a transponder module has only one port, the port number is always 0. For example, the client side interface identifier for a transponder module in subcard position 2 in slot 4 is transparent 4/2/0.

Wave Interfaces

The wave interface is the specific wavelength generated by a transponder module. The wave interface electrically connects to the client side transparent interface and optically connects to two wavepatch interfaces on a splitter protected line card motherboard (see Figure 2-1), or to one wavepatch interface on an unprotected line card motherboard (see Figure 2-2).

The naming convention for wave interfaces is as follows:

wave *slot/subcard*

Waveethernetphy Interfaces

The waveethernetphy interface is a colored interface that carries 2.5-Gbps or 10-Gbps Ethernet physical layer signals. This interface resides on the same card as the corresponding uncolored interface. It does not terminate Layer 2 or Layer 3 protocol operations.

The naming convention for the waveethernetphy interfaces on the 10-GE transponder module is as follows:

waveethernetphy *slot/subcard*

Wavepatch Interfaces

The wavepatch interface is the interface on the line card motherboard between the transponder modules and the mux/demux modules. The wave interfaces on the ITU side of the transponder modules connect to the wavepatch interfaces, which send the signal to the front panel of the line card motherboard. From the front panel connector, the wavepatch interface cross connects to the filter interface connector on a mux/demux module or a mux/demux motherboard, either directly or through the cross connect panel.

A splitter protected line card motherboard has two wavepatch interfaces for each subcard position and two MTP connectors for the wavepatch interfaces on its front panel. (See Figure 2-1.)

An unprotected line card motherboard has only one wavepatch interface per subcard position and only one MTP connector for the wavepatch interfaces on its front panel. (See Figure 2-2.)

The wavepatch interface operational state reflects the operational state of the corresponding wave interface. If the wave interfaces are operationally down, the corresponding wavepatch interfaces are operationally down. Conversely, if the wave interfaces are operationally up, then the wavepatch interfaces are up. However, the administrative states of the wave and wavepatch interfaces are independently tracked.

The naming convention for wavepatch interfaces is as follows:

wavepatch *slot/subcard/port*

On a splitter protected motherboard with two MTP connectors, the upper MTP connector on the front panel supports wavepatch *slot/subcard/0* interfaces and the lower MTP connector supports the wavepatch *slot/subcard/1* interfaces. On an unprotected motherboard, the MTP connector supports wavepatch *slot/subcard/0* interfaces.

Filter Interfaces

Each filter interface corresponds to an individual wavelength filter on the front panel of a mux/demux module. The filter interface cross connects a wavepatch interface on a line card motherboard to a wdm interface on the same mux/demux module (see Figure 2-1). This cross connection can be a direct connection between the line card motherboard and the mux/demux module or the mux/demux motherboard, or it can be a connection through the cross connect panel.

The naming convention for filter interfaces is as follows:

filter *slot/subcard/port*

The port numbers are 0 through 3 for 4-channel mux/demux modules, 0 through 7 for 8-channel mux/demux modules, and 0 through 31 for 32-channel mux/demux modules.

Wdm Interfaces

The wdm interface is the interface on the mux/demux module that receives the DWDM signal containing wavelengths to be dropped, or transmits the DWDM signal with added wavelengths. It represents the pairs of fibers (Tx and Rx) coming out of a mux/demux module. The wdm interface connects either to a wdm interface on another network node or, in the case of an add/drop mux/demux module, to a thru interface on another add/drop mux/demux module in the same slot (see Figure 2-1). The wdm interface can also connect to a thru interface on another shelf in a multiple shelf node.

The naming convention for wdm interfaces is as follows:

wdm *slot/subcard*

Thru Interfaces

The thru interface is the interface on the add/drop mux/demux module that sends the DWDM signal to, or receives it from, another add/drop mux/demux module without altering it. It represents the pairs of fibers (Tx and Rx) coming out of an add/drop mux/demux module. The thru interface connects the wdm or thru interface on another mux/demux module, either on the same slot or the other slot. The thru interface can also connect to a wdm interface on another shelf in a multiple shelf node.

The naming convention for thru interfaces is as follows:

thru *slot/subcard*

Wdmrelay Interfaces

The wdmrelay interface on a PSM (protection switch module) is a passive interface that represents a pair of fibers and connects the PSM to the wdm interface on a mux/demux module.

The naming convention for wdmrelay interfaces is as follows:

wdmrelay *slot/subcard/port*

Wdmsplit Interfaces

The wdmsplit interface on a PSM represents a pair of fibers and connects the trunk fiber. The PSM has two wdmsplit interfaces, one for the west direction and one for the east.

The naming convention for `wdmsplit` interfaces is as follows:

`wdmsplit slot/subcard/port`

The west interface is **`wdmsplit slot/subcard/0`** and the east interface is **`wdmsplit slot/subcard/1`**.

OSC Interfaces

The optional OSC provides management communications among the Cisco ONS 15540 ESPx systems in a network. The OSC is separate from the 32 data channels. The shelf can have two OSCs, one per mux/demux slot. Each OSC has two interfaces: one connection on the mux/demux motherboard and one on the mux/demux module that sends and receives the OSC wavelength on the network trunk (see Figure 2-1). Each interface represents the pairs of fibers (Tx and Rx).

The naming convention for the OSC interface on a mux/demux motherboard is as follows:

`wave slot`

The naming convention for the OSC interface on a mux/demux module is as follows:

`oscfiler slot/subcard`

The subcard position number for an `oscfiler` interface on a terminal mux/demux module is either 0 or 2 because the module occupies two subcard positions in the mux/demux motherboard.



Note

Only one mux/demux module per slot can have an OSC filter interface. For more information on hardware rules, refer to the *Cisco ONS 15540 ESPx Planning Guide*.

Ethernetdcc Interfaces

The `ethernetdcc` interfaces provide the communication path for the in-band message channel OAM messages between the 10-Gbps ITU trunk card and the CPU switch modules. The `ethernetdcc` interface connects the switch fabrics to the `waveethernetphy` interface.

The naming convention for `ethernetdcc` interfaces is as follows:

`ethernetdcc slot/subcard/port`

Each card has one `ethernetdcc` interface.

NME Interfaces

Each processor card has a Fast Ethernet interface, called an NME (network management Ethernet), for network management purposes. The NME interface on the active processor card is named `fastethernet 0` and the NME interface on the standby processor card is named `fastethernet-sby 0`.

Each NME interface has a unique MAC address. Also, you must configure each NME interface with a unique IP address. After a processor switchover, when standby processor card takes over as active, the IP and MAC addresses of the standby processor card are reinitialized to those of the active processor card.

**Note**

Network management system sessions and Telnet sessions are allowed on the NME interface on the active processor card (fastethernet 0) but not allowed on the NME interface on the standby processor card (fastethernet-sby 0).

Auxiliary Port Interfaces

Each processor card has an auxiliary port interface. You can use this interface for modem connections. This interface is named aux 0.

**Note**

Each Cisco ONS 15540 ESPx processor card has an ASE (aggregation shelf Ethernet) interface. This interface is not supported.

Configuration Overview

To configure your Cisco ONS 15540 ESPx systems and network, perform the following steps:

-
- Step 1** Select transponder modules, line card motherboards, mux/demux modules, and mux/demux motherboards to meet your requirements.
- For detailed information about the hardware components, refer to the *Cisco ONS 15540 ESPx Hardware Installation Guide*. For detailed information on system planning, refer to the *Cisco ONS 15540 ESPx Planning Guide*.
- Step 2** Insert the modules, motherboards, and processor cards into the chassis.
- For detailed information on hardware configuration rules, refer to the *Cisco ONS 15540 ESPx Planning Guide*.
- Step 3** Configure the NME ports on the active processor card and on the standby processor card, if present.
- For detailed information on configuring the NME port, see Chapter 3, “Initial Configuration.”
- Step 4** Cross connect the line card motherboards and mux/demux modules directly to each other or use the patch panels. Configure the patch connections with the CLI.
- For detailed information on cross connecting modules, refer to the *Cisco ONS 15540 ESPx Planning Guide*. For information on configuring patch connections with the CLI, see the “Configuring Patch Connections” section on page 4-21.
- Step 5** Connect the mux/demux modules with optical cables. If present, connect the OSC interface on the mux/demux motherboard to the OSC interface on a mux/demux module in the same slot and connect the PSM interfaces to trunk mux/demux module. Configure the patch connections with the CLI.
- For detailed information on cabling between mux/demux modules, refer to the *Cisco ONS 15540 ESPx Planning Guide*. For information on configuring patch connections with the CLI, see the “Configuring Patch Connections” section on page 4-21.
- Step 6** Verify the patch connections and cross connections using the **show patch** and **show connect** commands.
- For more information about the **show patch** and **show connect** commands, see the “Displaying Patch Connections” section on page 4-23 and the “About Cross Connections” section on page 4-24.

- Step 7** For all transparent interfaces in the shelf, configure either the protocol encapsulation or the clock rate for the client signal. Also, enable protocol monitoring for supported protocol encapsulations.
- For detailed information on interface configuration, see Chapter 4, “Configuring 2.5-Gbps Transponder Module Interfaces and Patch Connections.”
- Step 8** Configure APS.
- For detailed information on configuring APS, see Chapter 7, “Configuring APS.”
- Step 9** Configure processor card redundancy.
- For detailed information on processor card redundancy, see the “About Processor Card Redundancy” section on page 3-15.
- Step 10** Configure IP connectivity on the OSC for network management.
- For detailed information on configuring IP connectivity on the OSC, see the “Configuring IP on the OSC” section on page 11-9.
- Step 11** Configure CDP and the network topology.
- For detailed information on network monitoring, see Chapter 11, “Monitoring Your Network Topology”.
-



Initial Configuration

This chapter describes how to configure the Cisco ONS 15540 ESPx so it can be accessed by other devices. This chapter includes the following sections:

- About the Processor Card, page 3-1
- Starting Up the Cisco ONS 15540 ESPx, page 3-2
- Using the Console Ports, NME Ports, and Auxiliary Ports, page 3-2
- About Passwords, page 3-3
- Configuring IP Access on the NME Interface, page 3-3
- Configuring the Host Name, page 3-6
- About NTP, page 3-6
- Configuring NTP, page 3-7
- Configuring Security Features, page 3-8
- About Processor Card Redundancy, page 3-15
- Configuring Processor Card Redundancy, page 3-18
- About the Software Configuration Register, page 3-30
- Changing the Software Configuration Register, page 3-33
- About Fan Failure Shutdown, page 3-34
- Configuring Fan Failure Shutdown, page 3-35
- About Critical Temperature Shutdown, page 3-36
- Configuring Critical Temperature Shutdown, page 3-37

About the Processor Card

The processor card provides intelligence to the Cisco ONS 15540 ESPx. The processor card supports SNMP (Simple Network Management Protocol) and many MIBs (Management Information Bases).

The Cisco ONS 15540 ESPx uses 64-bit MIPS RM7000 processors running at 250 MHz. The processor has primary cache comprised of 16 KB for instructions and 16 KB for data. The secondary cache is 256 KB for both instructions and data. A third-level cache controller supports 512 KB, 1 MB, 2 MB, 4 MB, and 8 MB block write-through cache. Both the primary cache and the secondary cache are integrated onto the processor. The optional third-level cache is controlled through an on-chip cache controller.

The processor card supports a dual-height Flash memory Type II slot that can accommodate two Flash PC Cards or Flash disks.

The Cisco ONS 15540 ESPx supports redundant operation with dual processor cards. The processor cards reside in slots 6 and 7, the seventh and eighth slots from the left as you face the chassis. For more information, see the “About Processor Card Redundancy” section on page 3-15.

For more information on the processor card, refer to the *Cisco ONS 15540 ESPx Hardware Installation Guide*.

Starting Up the Cisco ONS 15540 ESPx

Before starting up the Cisco ONS 15540 ESPx, you should verify the following:

- The system is set for the correct AC (or DC) power voltages.
Refer to the *Cisco ONS 15540 ESPx Hardware Installation Guide* for correct power voltages.
- The cables are connected to the system.
- A console terminal is connected to the system.

Refer to the *Cisco ONS 15540 ESPx Hardware Installation Guide* for instructions.

When you start up the Cisco ONS 15540 ESPx, the CLI (command-line interface) prompts you to enter the initial configuration dialog. Answer **no** to this prompt:

```
Would you like to enter the initial dialog? [yes]: no
```

You see the following user EXEC prompt:

```
Switch>
```

You can now begin configuring the processor card.

Using the Console Ports, NME Ports, and Auxiliary Ports

You can configure the Cisco ONS 15540 ESPx from a direct console connection to the console port or remotely through its NME (network management Ethernet) port.

- If you are using a direct console connection, configure your terminal emulation program for 9600 baud, 8 data bits, no parity, and 1 stop bit.
- If you are using the NME port interface, you must assign an IP address to the interface (fastethernet 0).

For interface configuration instructions, see the “Configuring IP Access on the NME Interface” section on page 3-3.

For further details on configuring ports and lines for management access, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Modem Support

The auxiliary port of the Cisco ONS 15540 ESPx provides modem connection support. However, the hardware flow control signals are not available on the auxiliary port. The following settings on the modem are required:

- Enable auto answer mode.
- Suppress result codes.
- Disable hardware flow control.
- Ensure auxiliary port terminal characteristics (speed/stop bits/parity) match that of the modem.

You can configure your modem by setting the DIP switches on the modem itself or by setting them through terminal equipment connected to the modem. Refer to the user manual provided with your modem for the correct configuration information.

**Note**

Because there are no hardware flow control signals available on the auxiliary port, the auxiliary port terminal characteristics should match the modem settings.

For further details on configuring ports and modems for management access, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* and the *Cisco IOS Dial Services Configuration Guide*.

About Passwords

You can configure both an enable password and an enable secret password. For maximum security, the enable password should be different from the enable secret password.

Enable Password

The enable password is a nonencrypted password. It can contain any number of uppercase and lowercase alphanumeric characters. Give the enable password only to users permitted to make configuration changes to the Cisco ONS 15540 ESPx.

Enable Secret Password

The enable secret password is a secure, encrypted password. By setting an encrypted password, you can prevent unauthorized configuration changes. On systems running Cisco IOS, you must type in the enable secret password before you can access global configuration mode. You must type in the enable secret password to access boot ROM software.

An enable secret password contains from 1 to 25 uppercase and lowercase alphanumeric characters. The first character cannot be a number. Spaces are valid password characters. Leading spaces are ignored; trailing spaces are recognized.

You will configure passwords in the next section, “Configuring IP Access on the NME Interface”.

Configuring IP Access on the NME Interface

The Fast Ethernet interface, or NME, on the active processor card, named *fastethernet 0*, is the management interface that allows multiple, simultaneous Telnet or SNMP network management sessions.

You can remotely configure the Cisco ONS 15540 ESPx through the Fast Ethernet interface, but first you must configure an IP address so that the active processor card is reachable. There are two ways to configure the NME interface: manually from the CLI or by copying the configuration from the BOOTP server into NVRAM.

For information on configuring the NME interface on the standby processor card, *fastethernet-sby 0*, refer to the *Cisco ONS 15540 ESPx Software Upgrade Guide*.



Note Before you begin to manually configure an NME interface, obtain its IP address and IP subnet mask. Also make sure the console cable is connected to the console port.

To configure IP access on the NME port *fastethernet 0* from the CLI, perform these steps from the console interface:

	Command	Purpose
Step 1	Switch> enable Switch#	Enters privileged EXEC mode.
Step 2	Switch# show hardware	Verifies the installed hardware part numbers and serial numbers.
Step 3	Switch# configure terminal Switch(config)#	Enters global configuration mode.
Step 4	Switch(config)# enable password <i>password</i>	Sets the enable password. See the “About Passwords” section on page 3-3.
Step 5	Switch(config)# enable secret <i>password</i>	Specifies an enable secret password. Once set, the enable secret password must be entered to gain access to global configuration mode.
Step 6	Switch(config)# interface fastethernet 0 Switch(config-if)#	Enters interface configuration mode on interface <i>fastethernet 0</i> , the NME port on the active processor card.
Step 7	Switch(config-if)# ip address <i>ip-address</i> <i>subnet-mask</i>	Specifies the IP address and IP subnet mask for the management port interface.
Step 8	Switch(config-if)# speed { 10 100 auto }	Specifies the transmission speed. The default is auto (autonegotiation).
Step 9	Switch(config-if)# duplex { auto full half }	Specifies the duplex mode. The default is auto (autonegotiation).
Step 10	Switch(config-if)# exit Switch(config)#	Returns to global configuration mode.
Step 11	Switch(config)# ip default-gateway <i>ip-address</i>	Specifies the address of the default IP gateway node.
Step 12	Switch(config)# line vty <i>line-number</i> Switch(config-line)#	Enters line configuration mode for virtual terminal connections. Commands entered in this mode control the operation of Telnet sessions.
Step 13	Switch(config-line)# password <i>password</i>	Specifies a password for Telnet sessions.

	Command	Purpose
Step 14	Switch(config-line)# end Switch#	Returns to privileged EXEC mode.
Step 15	Switch# copy system:running-config nvram:startup-config	Saves the configuration changes to NVRAM.

The Cisco ONS 15540 ESPx NME interface should now be operating correctly.



Note If a processor card switchover occurs, you can use the same IP address to access the other processor card after it becomes active.



Note In a dual shelf node configuration, perform these steps on the NME interfaces on both shelves in the node.

Displaying the NME Interface Configuration

To display the configuration of the NME interface, use the following EXEC command:

Command	Purpose
show interfaces fastethernet 0	Displays the NTP status.

Example

```
Switch# show interfaces fastethernet 0
→ FastEthernet0 is up, line protocol is up
   Hardware is AmdFE, address is 0000.1644.28ea (bia 0000.1644.28ea)
→   Internet address is 172.20.54.152/24
   MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
   Encapsulation ARPA, loopback not set
   Keepalive set (10 sec)
→   Half-duplex, 10Mb/s, 100BaseTX/FX
   ARP type: ARPA, ARP Timeout 04:00:00
   Last input 00:00:00, output 00:00:00, output hang never
   Last clearing of "show interface" counters never
   Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
   Queueing strategy: fifo
   Output queue :0/40 (size/max)
   5 minute input rate 3000 bits/sec, 6 packets/sec
   5 minute output rate 1000 bits/sec, 3 packets/sec
     36263 packets input, 3428728 bytes
       Received 17979 broadcasts, 0 runts, 0 giants, 0 throttles
       0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
       0 watchdog
       0 input packets with dribble condition detected
     20363 packets output, 4279598 bytes, 0 underruns
       0 output errors, 8 collisions, 0 interface resets
       0 babbles, 0 late collision, 72 deferred
       0 lost carrier, 0 no carrier
       0 output buffer failures, 0 output buffers swapped out
```

Displaying the Operating Configurations

You can display the configuration file when you are in privileged EXEC (enable) mode.

- To see the current operating configuration, enter the following command at the enable prompt:

```
Switch# more system:running-config
```

- To see the configuration saved in NVRAM, enter the following command:

```
Switch# more nvram:startup-config
```

If you made changes to the configuration, but did not yet write the changes to NVRAM, the contents of the running-config file will differ from the contents of the startup-config file.

Configuring the Host Name

In addition to passwords and an IP address, your initial configuration should include the host name to make it easier to configure and troubleshoot the Cisco ONS 15540 ESPx. To configure the host name, perform the following steps:

	Command	Purpose
Step 1	Switch# configure terminal Switch(config)#	Enters global configuration mode.
Step 2	Switch(config)# hostname name	Specifies a system name.
Step 3	<i>name</i> (config)# end <i>name</i> #	Returns to privileged EXEC mode. The prompt indicates that the host name has been set to the new name.
Step 4	<i>name</i> # copy system:running-config nvram:startup-config	Saves your configuration changes to NVRAM.



Note

The host name is also synchronized with the standby processor card. The host name prompt on the standby processor card appears with “sby-” as a prefix.

Example

The following example shows how to configure a new host name, beginning in privileged EXEC mode:

```
Switch# configure terminal
Switch(config)# hostname ONS15540
ONS15540(config)# end
ONS15540# copy system:running-config nvram:startup-config
```

About NTP

The NTP (Network Time Protocol) is a utility for synchronizing system clocks over the network, providing a precise time base for networked workstations and servers. In the NTP model, a hierarchy of primary and secondary servers pass timekeeping information by way of the Internet to cross-check clocks and correct errors arising from equipment or propagation failures.

An NTP server must be accessible by the client switch. NTP runs over UDP (User Datagram Protocol), which in turn runs over IP. NTP is documented in RFC 1305. All NTP communication uses UTC (Coordinated Universal Time), which is the same as Greenwich Mean Time. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within a millisecond of one another.

NTP uses a stratum to describe how many NTP hops away a machine is from an authoritative time source. A stratum 1 time server has a radio or atomic clock directly attached, a stratum 2 time server receives its time from a stratum 1 time server, and so on. A machine running NTP automatically chooses as its time source the machine with the lowest stratum number that it is configured to communicate with through NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

NTP has two ways to avoid synchronizing to a machine whose time might be ambiguous:

- NTP never synchronizes to a machine that is not synchronized itself.
- NTP compares the time reported by several machines and does not synchronize to a machine whose time is significantly different from the others, even if its stratum is lower.

The communications between machines running NTP, known as associations, are usually statically configured; each machine is given the IP address of all machines with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of machines with an association.

The Cisco implementation of NTP does not support stratum 1 service; it is not possible to connect to a radio or atomic clock. We recommend that you obtain the time service for your network from the public NTP servers available in the IP Internet. If the network is isolated from the Internet, the Cisco NTP implementation allows a machine to be configured so that it acts as though it is synchronized using NTP, when in fact it has determined the time using other means. Other machines then synchronize to that machine using NTP.

A number of manufacturers include NTP software for their host systems, and a version for systems running UNIX and its various derivatives is also publicly available. This software allows host systems to be time-synchronized as well.

Configuring NTP

NTP services are enabled on all interfaces by default. You can configure your Cisco ONS 15540 ESPx in either of the following NTP associations:

- Peer association—This system either synchronizes to the other system or allows the other system to synchronize to it.
- Server association—This system synchronizes to the other system, and not the other way around.

From global configuration mode, use the following procedure to configure NTP in a server association that transmits broadcast packets and periodically updates the calendar:

	Command	Purpose
Step 1	Switch(config)# ntp update-calendar	Updates hardware calendar with NTP time.
Step 2	Switch(config)# ntp server ip-address	Forms a server association with another system. You can specify multiple associations.

	Command	Purpose
Step 3	Switch(config)# end Switch#	Returns to privileged EXEC mode.
Step 4	Switch# copy system:running-config nvram:startup-config	Saves your configuration changes to NVRAM.

For information on other optional NTP configurations, see the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Displaying the NTP Configuration

To view the current NTP configuration and status, use the following EXEC command:

Command	Purpose
show ntp status	Displays the NTP status.

Example

The following example shows the NTP configuration and status:

```
Switch# show ntp status
Clock is synchronized, stratum 4, reference is 198.92.30.32
nominal freq is 250.0000 Hz, actual freq is 249.9999 Hz, precision is 2**24
reference time is B6C04F19.41018C62 (18:21:13.253 UTC Thu Feb 27 1997)
clock offset is 7.7674 msec, root delay is 113.39 msec
root dispersion is 386.72 msec, peer dispersion is 1.57 msec
```

Configuring Security Features

The Cisco ONS 15540 ESPx supports the following Cisco IOS software security features:

- AAA (authentication, authorization, and accounting)
- Kerberos
- RADIUS
- TACACS+
- SSH (Secure Shell)
- Traffic filters and firewalls
- Passwords and privileges

Configuring AAA

This section describes the AAA features supported by the Cisco ONS 15540 ESPx.

Configuring Authentication

To configure AAA authentication, perform the following tasks:

-
- Step 1** Enable AAA by using the **aaa new-model** global configuration command.
 - Step 2** Configure security protocol parameters, such as RADIUS, TACACS+, or Kerberos if you are using a security server. Refer to the “Configuring RADIUS” chapter, the “Configuring TACACS+” chapter, or the “Configuring Kerberos” chapter in the *Cisco IOS Security Configuration Guide*.
 - Step 3** Define the method lists for authentication by using an AAA authentication command.
 - Step 4** Apply the method lists to a particular interface or line, if required.
-

Refer to the “Configuring Authentication” chapter in the *Cisco IOS Security Configuration Guide*.

Configuring Authorization

The AAA authorization feature enables you to limit the services available to a user. When AAA authorization is enabled, the network access server uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's session. Once this is done, the user is granted access to a requested service only if the information in the user profile allows it.

Refer to the “Configuring Authorization” chapter in the *Cisco IOS Security Configuration Guide*.

Configuring Accounting

The AAA accounting feature enables you to track the services that users are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the network access server reports user activity to the TACACS+ or RADIUS security server (depending on which security method you have implemented) in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, and auditing.

Refer to the “Configuring Accounting” chapter in the *Cisco IOS Security Configuration Guide*.

Configuring Kerberos

For hosts and the KDC in your Kerberos realm to communicate and mutually authenticate, you must identify them to each other. To do this, you add entries for the hosts to the Kerberos database on the KDC and add SRVTAB files generated by the KDC to all hosts in the Kerberos realm. You also make entries for users in the KDC database.

Refer to the “Configuring Kerberos” chapter in the *Cisco IOS Security Configuration Guide*.

Configuring RADIUS

RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on Cisco ONS 15540 ESPx systems and send authentication requests to a central RADIUS server that contains all user authentication and network service access information. RADIUS is a fully open protocol, distributed in source code format, that can be modified to work with any security system currently available.

To configure RADIUS on your Cisco router or access server, perform the following tasks:

-
- Step 1** Use the **aaa new-model** global configuration command to enable AAA. AAA must be configured if you plan to use RADIUS. Refer to the “AAA Overview” chapter in the *Cisco IOS Security Configuration Guide*.
- Step 2** Use the **aaa authentication global** configuration command to define method lists for RADIUS authentication. Refer to the “Configuring Authentication” chapter in the *Cisco IOS Security Configuration Guide*.
- Step 3** Use **line** and **interface** commands to enable the defined method lists to be used. Refer to the “Configuring Authentication” chapter in the *Cisco IOS Security Configuration Guide*.
-

The following configuration tasks are optional:

- You may use the **aaa group server** command to group selected RADIUS hosts for specific services.
- You may use the **aaa dnis map** command to select RADIUS server groups based on DNIS number. To use this command, you must define RADIUS server groups using the **aaa group server** command.
- You may use the **aaa authorization** global command to authorize specific user functions. Refer to the “Configuring Authorization” chapter in the *Cisco IOS Security Configuration Guide*.
- You may use the **aaa accounting** command to enable accounting for RADIUS connections. Refer to the “Configuring Accounting” chapter in the *Cisco IOS Security Configuration Guide*.
- You may use the dialer **aaa interface** configuration command to create remote site profiles that contain outgoing call attributes on the AAA server.

Refer to the “Configuring RADIUS” chapter in the *Cisco IOS Security Configuration Guide*.

Configuring TACACS+

To configure your router to support TACACS+, perform the following tasks:

-
- Step 1** Use the **aaa new-model** global configuration command to enable AAA. AAA must be configured if you plan to use TACACS+. Refer to the “AAA Overview” chapter in the *Cisco IOS Security Configuration Guide*.
- Step 2** Use the **tacacs-server host** command to specify the IP address of one or more TACACS+ daemons. Use the **tacacs-server key** command to specify an encryption key that is used to encrypt all exchanges between the network access server and the TACACS+ daemon. This same key must also be configured on the TACACS+ daemon.
- Step 3** Use the **aaa authentication** global configuration command to define method lists that use TACACS+ for authentication. Refer to the “Configuring Authentication” chapter in the *Cisco IOS Security Configuration Guide*.
- Step 4** Use **line** and **interface** commands to apply the defined method lists to various interfaces. Refer to the “Configuring Authentication” chapter in the *Cisco IOS Security Configuration Guide*.
- Step 5** If needed, use the **aaa authorization** global command to configure authorization for the network access server. Unlike authentication, which can be configured per line or per interface, authorization is configured globally for the entire network access server. Refer to the “Configuring Authorization” chapter in the *Cisco IOS Security Configuration Guide*.

- Step 6** If needed, use the **aaa accounting** command to enable accounting for TACACS+ connections. Refer to the “Configuring Accounting” chapter in the *Cisco IOS Security Configuration Guide*.

Refer to the “Configuring TACACS+” chapter in the *Cisco IOS Security Configuration Guide*.

Configuring Secure Shell

The preferred method of administering the system is through a Telnet session. However, using Telnet can cause security issues that include session hijacking, sniffing, and man-in-the-middle attacks. These attacks might be stopped using the Secure Shell (SSH) protocol and application, which the system supports. SSH is an application and protocol that secures the sessions using standard cryptographic mechanisms. Two versions of SSH are currently available, SSHv1 and SSHv2.

SSH runs on top of a reliable transport layer, such as TCP/IP, and provides strong authentication and encryption capabilities. SSH allows you to log in to a host over a network, execute commands remotely, and move files from one host to another. The requirements are:

- Any host that needs an incoming secure connection must have the SSH daemon (or server) running.
- The SSH client is required to initiate a connection to the remote host.

The Cisco IOS implementation of the SSH server on the system provides the following:

- Secure incoming connections
- Remote EXEC session connections to the system
- DES, 3DES, and AES (128, 192, and 256 bit) encryption
- Username and password authentication using the existing Cisco IOS AAA authentication functions
- SSHv1 and SSHv2

To configure SSH on the system, perform the following steps in global EXEC mode:

	Command	Purpose
Step 1	Switch(config)# hostname <i>name</i>	Sets the host name.
Step 2	Switch(config)# ip domain-name <i>name</i>	Configures the system IP domain name.
Step 3	Switch(config)# crypto key {generate [usage-keys [modulus modulus-value]] zeroize} rsa	Generates an RSA key pair.
Step 4	Switch(config)# ip ssh version {version-number}	Configures the SSH server version

Example

The following example shows how to configure the SSH client and start the SSH server:

```
Switch(config)# hostname
Switch(config)# ip domain-name cisco.com
Switch(config)# crypto key generate rsa
Switch(config)#
```

To start SSH client functionality on the system, perform the following step:

Command	Purpose
Switch# ssh [-l <i>userid</i>] [-c { des 3des aes128-cbc aes192-cbc aes256-cbc }] [-m { hmac-md5-128 hmac-md5-96 hmac-sha1-160 hmac-sha1-96 }] [-o -p <i>portnumber</i>] [-v { 1 2 }] [<i>ip_address</i> <i>hostname</i>] [<i>command(command(command...))</i>]	Starts the SSH client. <i>Command</i> specifies the Cisco IOS command that you want to run on the remote networking device. If the remote host is not running Cisco IOS software, this may be any command recognized by the remote host. If the command includes spaces, you must enclose the command in quotation marks

**Note**

You can run the SSH client configuration from any EXEC configuration level.

Displaying and Disconnecting SSH

To display the SSH utilization, use the following privileged EXEC commands:

Command	Purpose
show ssh	Displays SSH connection information.
disconnect ssh <i>session-id</i>	Disconnects an SSH session.
show ip ssh	Displays the SSH configuration.

Examples

The following example shows how to display the SSH connection information:

```
Switch# show ssh
Connection      Version Encryption      State      Username
0               1.5        3DES              Session started      sriram
Connection Version Mode Encryption Hmac      State      Username
1             2.0      IN  aes128-cbc hmac-md5   Session started      aarun
1             2.0      OUT aes128-cbc hmac-md5   Session started      aarun
```

The following example clears the outgoing SSH connection 0 using the **disconnect ssh** command:

```
Switch# disconnect ssh 0

[Connection to 10.13.1.98 closed by foreign host]
Switch#
```

The following example shows how to display the SSH configuration:

```
Switch# show ip ssh
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
```

Testing the System Management Functions

This section describes the commands used to monitor and display the system management functions.

Displaying Active Processes

To display information about the active processes, use the following privileged EXEC commands:

Command	Purpose
<code>show processes</code>	Displays active process statistics.
<code>show processes cpu</code>	Displays active process CPU utilization.
<code>show processes memory</code>	Displays active process memory utilization.

Displaying Protocols

To display the configured protocols, use the following privileged EXEC command:

Command	Purpose
<code>show protocols type card/subcard/port</code>	Displays the global and interface-specific status of any configured Level 3 protocol.

Displaying Stacks

The `show stacks` command output includes the reason for the last system reboot. If the system was reloaded because of a system failure, a saved system stack trace is displayed. This information is useful only to Cisco engineers analyzing crashes in the field. It is included here in case you need to read the displayed statistics to an engineer over the phone.

To monitor the stack utilization of processes and interrupt routines, use the following privileged EXEC command:

Command	Purpose
<code>show stacks number</code>	Displays system stack trace information.

Example

The following example displays system stack trace information.

```
Switch# show stacks
Minimum process stacks:
Free/Size   Name
5712/6000   CDP BLOB
8712/9000   cdp init process
8600/12000  Init
5432/6000   RADIUS INITCONFIG
9208/12000  Exec

Interrupt level stacks:
Level   Called Unused/Size Name
1       463487 8136/9000 NME/Backplane/PCMCIA interrupts
2       0       9000/9000 DMA/Timer Interrupt
3       10172321 8536/9000 Console Uart
4       0       9000/9000 GT/IOFPGA Error interrupts
5       0       9000/9000 OIR Intr
6       0       9000/9000 ARB Intr
7       86841  8120/9000 APS Intr
9       43168966 8552/9000 NMI Interrupt Handler
```

Displaying Environment

To display temperature and voltage information on the Cisco ONS 15540 ESPx console, use the following EXEC command:

Command	Purpose
show environment	Displays temperature and voltage information.

Checking Basic Connectivity

To diagnose basic network connectivity on the Cisco ONS 15540 ESPx, use the following privileged EXEC commands:

Command	Purpose
show interface { transparent <i>slot/subcard/port</i> wave <i>slot/subcard</i> wavepatch <i>slot/subcard/port</i> }	Displays the interface as up and in the correct state and proper counters are incrementing. There are no error counter incrementing.
show facility-alarm status	Displays alarms in the system.
show interface { osc slot etherdcc <i>slot/subcard/port</i> }	Displays management and message channel status.

Configuring Traffic Filters and Firewalls

The Cisco ONS 15540 ESPx supports the traffic filter and firewall features provided by Cisco IOS.

Traffic filters provide basic traffic filtering capabilities with access control lists (also referred to as *access lists*). Access lists can be configured for all routed network protocols (IP, AppleTalk, and so on) to filter the packets of those protocols as the packets pass through a system. You can configure access lists on your Cisco ONS 15540 ESPx to control access to a network, preventing certain traffic from entering or exiting a network.

Firewalls are networking devices that control access to your organization's network assets. You can position firewalls to control access at the entrance points into your network, or to control access to a specific part of your network.

For more information on traffic filtering and firewalls, refer to the *Cisco IOS Security Configuration Guide*.

Configuring Passwords and Privileges

Using passwords and assigning privilege levels is a simple way of providing terminal access control in your network. You can configure up to 16 different privilege levels and assign each level to a password. For each privilege level you define a subset of Cisco IOS commands that can be executed. You can use these different levels to allow some users the ability to execute all Cisco IOS commands, and to restrict other users to a defined subset of commands.

Refer to the “Configuring Passwords and Privileges” part in the *Cisco IOS Security Configuration Guide*.

About Processor Card Redundancy

The Cisco ONS 15540 ESPx supports fault tolerance by allowing the standby processor card to take over if the active processor card fails. This standby, or redundant, processor card runs in hot-standby state. In hot-standby state, the standby processor card is partially booted with Cisco IOS software, but no configuration is loaded.

At the time of a switchover from the active processor card, the standby processor card becomes active and loads the configuration as follows:

- If the running configuration file on the active and standby processor cards match, the new active processor card uses the running configuration file.
- If the running configuration file on the new active processor card is missing or invalid, the new active processor card uses the startup configuration file in its NVRAM (not the NVRAM of the former active processor card).

The former active processor card then reloads and becomes the standby processor card.



Note

If the standby processor card is unavailable, the system reports a minor alarm. Use the **show facility-alarm status** command to display the redundancy alarm status.

When the Cisco ONS 15540 ESPx is powered on, the two processor cards arbitrate to determine which is the active processor card and which is the standby processor card. The following rules apply during initial arbitration:

- The active processor at the time the system is powered off continues as the active processor when the system is powered on.
- If the active processor card cannot boot its software image, the standby processor card takes over as the active processor card within three minutes, allowing you to manually correct the problem with the former active processor card.
- If none of the above conditions is true, the processor card in slot 6 becomes the active processor card.

During normal operation, the active processor card boots completely. The standby processor card partially boots, stopping short of parsing the configuration. From this point, the active and standby processor cards communicate periodically to synchronize any system configuration changes.

Table 3-1 describes the five processor card hardware states.

Table 3-1 Processor Card Hardware States

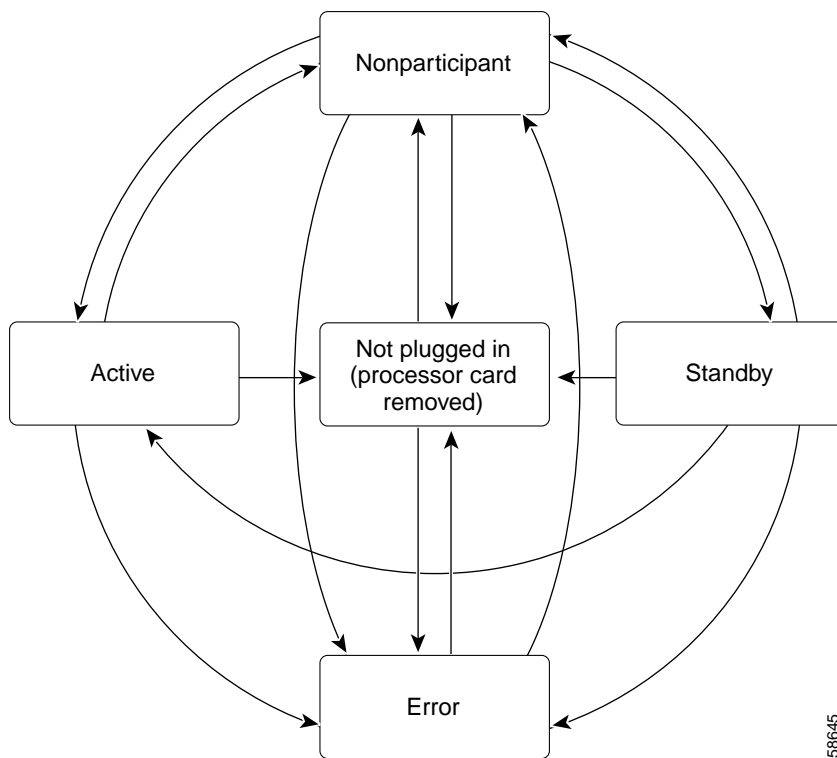
State	Description
Active	Processor card is currently providing clock signals and control for all system modules. The active processor card responds to the configured management IP address.
Standby	Processor card is partially booted in hot-standby state waiting to switch over when the active processor card fails, when it is rebooted or removed, or when a manual switchover is requested.
Nonparticipant	Processor card is in ROMMON mode, or is in the process of booting, or has not yet reached the hot-standby state. Manual switchovers are rejected unless the force option is used.

Table 3-1 Processor Card Hardware States (continued)

State	Description
Not plugged in	Processor card slot is empty.
Error	Processor card is present but either the interprocess arbitration interface is not functioning or the processor card is not fully seated in the chassis slot.

Figure 3-1 shows the valid hardware transition states for a system with redundant processor cards.

Figure 3-1 Processor Card State Transition Diagram



In response to redundancy events, such as switchovers and reboots of the active processor card, the software transitions through a series of software redundancy states. Table 3-2 lists some of the significant software states.

Table 3-2 Processor Card Software States

State	Description
Disabled	The standby processor card is not yet running the system image or is in maintenance mode.
Standby cold	The standby processor card is running the system image but has not begun to synchronize data from the active processor card.

Table 3-2 Processor Card Software States (continued)

State	Description
Standby hot	The standby processor card has fully synchronized the configuration and other data from the active processor card. It will remain in the hot-standby state until a switchover occurs.
Active	The processor card is in the active hardware state and has completed all switchover or initial bootup processing. It is fully ready to control the system.

Redundant Operation Requirements

For fully redundant operation, the following requirements must be met:

- Two processor cards are required.
- The processor cards must have identical hardware configurations. This includes variables such as DRAM size, and so on.
- Both processor cards must have the same functional image.
- Both processor cards must be running compatible system images. System images are compatible across one major release.
- Both the running and startup configurations are automatically synchronized between the processor cards.
- Both processor cards must be set to autoboot (a default setting).

If these requirements are met, the Cisco ONS 15540 ESPx runs in redundant mode by default. If they are not met, the system is conditionally redundant.



Note

For detailed information on updating system images, see the refer to the *Cisco ONS 15540 ESPx Software Upgrade Guide*.

Conditions Causing a Switchover from the Active Processor Card

The following conditions can cause a switchover from the active processor card to the standby processor card:

- The active processor card is removed or swapped. When the processor card functioning as the active processor card is removed, the standby processor card takes over. The Cisco ONS 15540 ESPx is nonredundant until a second processor card is inserted.
- The active processor card is rebooted. When a processor card functioning as the active processor card is rebooted, it relinquishes its active role if the standby processor card has reached the hot-standby state.
- The active processor card fails. The standby processor card takes over as the active processor card, using the last synchronized running configuration file (or the last saved startup configuration file if the running configuration file synchronization was disabled or failed).
- A switchover is manually forced with the **redundancy switch-activity** command.

Configuring Processor Card Redundancy

This section describes how to configure processor card redundancy for your Cisco ONS 15540 ESPx.


Note

The initial default configuration supports processor card redundancy and database synchronization with no manual configuration required.

Forcing a Switchover from Privileged EXEC Mode

You can manually force the standby processor card to take over as the active processor card from privileged EXEC mode. To force a switchover from privileged EXEC mode, enter the following command on the active processor card CLI:

Command	Purpose
<code>redundancy switch-activity [force]</code>	Causes a processor card switchover. If the standby processor card has not reached the hot-standby software state, use the force option.

As long as you have not changed the default configuration register setting from autoboot, the standby processor card (formerly the active processor card) automatically boots until it reaches the hot-standby state.


Note

Data transmission through the system is not affected by a processor card switchover.

Example

The following example shows how to manually cause a processor card switchover from privileged EXEC mode:

```
Switch# redundancy switch-activity
This will reload the active unit and force a switch of activity [confirm] y
Preparing to switch activity

00:12:05: %SYS-5-RELOAD: Reload requested
<Information deleted>
```

Forcing a Switchover from ROM Monitor Mode

You can manually force the standby processor card to take over as the active processor card ROM monitor mode. To force a switchover from ROM monitor mode, enter the following commands on the active processor card CLI:

Command	Purpose
<code>switchover</code>	Causes a processor card reset and switchover. The processor card stays in ROM monitor mode.

**Note**

Using the **reset** command in ROM monitor mode on the active processor CLI under normal conditions does not cause a switchover.

Example

The following example shows how to manually cause a processor card switchover from ROM monitor mode:

```
<Information deleted>
```

```
→ This CPU is ACTIVE (sev=0), peer CPU is NON-PARTICIPANT (sev=2)
MANHATTAN_OPTICAL platform with 131072 Kbytes of main memory

rommon 1 > switchover
System Bootstrap, Version 12.1(20010726:234219) [ffrazer-lh4 102], DEVELOPMENT S
SOFTWARE
Copyright (c) 1994-1999 by cisco Systems, Inc.
Flash size is 16777216

Reset Reason Register = RESET_REASON_SW_NMI (0x4)

Reset type 0x2

Reading monitor variables from NVRAM
Running reset I/O devices
Enabling interrupts

Initializing TLB

Initializing cache

Initializing required TLB entries
Initializing main memory

SDRAM DIMM size 67108864

Sizing NVRAM

Initializing PCMCIA controller

Initializing SRC FPGA
CPU arbitration

→ This CPU is NON-PARTICIPANT (sev=2), peer CPU is ACTIVE (sev=0)
MANHATTAN_OPTICAL platform with 131072 Kbytes of main memory

rommon 1 >
```

Configuring Autoboot

If you have changed the default configuration register value from autoboot, you can change it back by performing the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# config-register 0x2102	Sets the configuration register for autoboot. ¹
Step 2	Switch(config)# boot system bootflash:filename	Sets the BOOT environment variable. This variable specifies the location and name of the system image file to use when automatically booting the system.
Step 3	Switch(config)# end Switch#	Returns to privileged EXEC mode.
Step 4	Switch# copy system:running-config nvram:startup-config	Saves the configuration to NVRAM. The new configuration register value takes effect after the next system reload.

1. This is the default configuration register setting. For details on using the configuration register to set boot parameters, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*.



Note

If the standby processor card remains in ROM monitor mode, you can manually boot the processor card using a system image either on the bootflash or on a Flash PC Card.

Example

The following example shows how to configure the Cisco ONS 15540 ESPx to autoboot using the first valid file on the Flash PC Card in slot 0:

```
Switch(config)# config-register 0x2102
Switch(config)# boot system flash slot0:
Switch(config)# end
Switch# copy system:running-config nvram:startup-config
```

Displaying the Autoboot Configuration

To display the configuration register value, use the following EXEC command:

Command	Purpose
show version	Displays the configuration register value.
show bootvar	Displays the configuration register value.

Example

The following example shows the contents of the configuration register:

```
Switch# show version
Cisco Internetwork Operating System Software
IOS (tm) ONS-15540 Software (manopt-M0-M), Experimental Version 12.1(20010221:0)
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Tue 20-Feb-01 18:40 by lthanvan
Image text-base: 0x60010968, data-base: 0x604D8000

ROM: System Bootstrap, Version 12.1(20010204:232442) [vsankar-alarm_fix 106], DE
BOOTFLASH: M1540-ODS Software (manopt-M0-M), Experimental Version 12.1(20001229)
```

```

M1 uptime is 1 minute
System returned to ROM by power-on
System image file is "tftp://171.69.1.129//tftpboot/lthanvan/manopt-m0-mz"

cisco (QUEENS-CPU) processor with 98304K/32768K bytes of memory.
R7000 CPU at 234Mhz, Implementation 39, Rev 2.1, 256KB L2, 2048KB L3 Cache

Last reset from unexpected value
2 Ethernet/IEEE 802.3 interface(s)
509K bytes of non-volatile configuration memory.

16384K bytes of Flash internal SIMM (Sector size 64K).
→ Configuration register is 0x2102

```

The following example shows the contents of the boot variable:

```

→ Switch# show bootvar
BOOT variable = bootflash:ons15540-i-mz.1;
CONFIG_FILE variable =
BOOTLDR variable =
Configuration register is 0x2

Standby auto-sync startup config mode is on

Standby auto-sync running config mode is on

```

Synchronizing the Configurations

During normal operation, the startup and running configurations are synchronized by default between the two processor cards. In the event of a switchover, the new active processor card uses the current running configuration. Configurations are synchronized either manually from the CLI using the **redundancy manual-sync** command or automatically following configuration changes input from the CLI or from SNMP if automatic synchronization is enabled.

Synchronizing Configurations Manually

To immediately synchronize the configurations used by the two processor cards, use the following privileged EXEC command on the active processor card:

Command	Purpose
redundancy manual-sync {startup-config running-config both}	Immediately synchronizes the configuration.

Example

The following example shows how to manually synchronize the running configuration:

```
Switch# redundancy manual-sync running-config
```

Enabling and Disabling Automatic Synchronization

You can enable and disable automatic synchronization of the running configuration and the startup configuration between the two processor cards. Automatic synchronization ensures that, when a switchover occurs, the standby processor card has the most recent configuration information.

**Note**

By default, the Cisco ONS 15540 ESPx automatically synchronizes the running configuration and the startup configuration between the two processor cards.

Table 3-3 lists the events that cause the automatic synchronization of the configuration files.

Table 3-3 Synchronization Events for Configuration Files

Filename	When Synchronized
running-config	Upon exiting from global configuration mode in the CLI, or within 5 seconds after an SNMP message that changes the configuration
startup-config	When a new configuration is copied to NVRAM on the active processor card

To enable or disable the system to automatically synchronize the configurations on both processor cards, perform the following steps on the active processor card, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# redundancy Switch(config-red)#	Enters redundancy configuration mode.
Step 2	Switch(config-red)# [no] auto-sync running-config	Enables or disables synchronization of the running configuration when it is updated. The default state is enabled.
Step 3	Switch(config-red)# [no] auto-sync startup-config	Enables or disables synchronization of the startup configuration when it is updated. The default state is enabled.

Example

The following example shows how to disable automatic synchronization of the running configuration:

```
Switch(config)# redundancy
Switch(config-red)# no auto-sync running-config
Switch(config-red)# end
Switch# copy system:running-config nvram:startup-config
```

Configuring Maintenance Mode

You can configure the Cisco ONS 15540 ESPx to enter the redundancy maintenance mode. Configuration synchronizations and standby processor card fault reporting are suppressed in maintenance mode. Upon exiting maintenance mode and reverting to redundant mode, the standby processor card is rebooted to bring it back to the hot-standby state.

**Note**

When the system is in maintenance mode, switchovers only occur by entering the **redundancy switch-activity force** command, or physically removing the active processor card.

To configure maintenance mode, perform the following commands, beginning in global configuration mode:

Command	Purpose
Switch(config)# redundancy Switch(config-red)#	Enters redundancy configuration mode.
Switch(config-red)# maintenance-mode	Configures the system in maintenance mode.

Example

The following example shows how to configure redundancy maintenance mode:

```
Switch(config)# redundancy
Switch(config-red)# maintenance-mode
This command will place the system in SIMPLEX mode [confirm] y
```

Displaying the Processor Card Redundancy Configuration and Status

To display the processor card redundancy configuration and status, use the following privileged EXEC commands:

Command	Purpose
show redundancy summary	Displays the redundancy configuration and status.
show redundancy capability	Displays capabilities of the active and standby processor cards and the software version that is running.
show redundancy running-config-file	Displays the running configuration file on the standby processor card. Note This command is only available on a terminal connected to the standby processor card.

Examples

The following example shows the processor card redundancy configuration and status:

```
Switch# show redundancy summary

Redundant system information
-----
Available Uptime:           3 days, 4 hours, 35 minutes
Time since last switchover: 10 hours, 30 minutes
Switchover Count:          1

Inter-CPU Communication State:UP
Last Restart Reason:       Switch over
Software state at switchover: ACTIVE

Last Running Config sync:   2 hours, 18 minutes
Running Config sync status: In Sync
Last Startup Config sync:   6 hours, 4 minutes
Startup Config sync status: In Sync

This CPU is the Active CPU.
-----
Slot:                       7
```

```

Time since CPU Initialized: 22 hours, 33 minutes
Image Version:            ONS-15540 Software(ONS15540-I-M),...
Image File:               bootflash:ons15540-i-mz.010727
Software Redundancy State: ACTIVE
Hardware State:           ACTIVE
Hardware Severity:        0

```

Peer CPU is the Standby CPU.

```

-----
Slot:                      6
Time since CPU Initialized: 10 hours, 29 minutes
Image Version:             ONS-15540 Software(ONS15540-I-M),...
Image File (on sby-CPU):  bootflash:ons15540-i-mz.010727
Software Redundancy State: STANDBY HOT
Hardware State:            STANDBY
Hardware Severity:         0

```

The following example shows the processor card capabilities:

```

Switch# show redundancy capability
CPU capability support

```

Active CPU	Sby CPU	Sby Compat	CPU capability description
96 MB	96 MB	OK	CPU DRAM size
32 MB	32 MB	OK	CPU PMEM size
512 KB	512 KB	OK	CPU NVRAM size
16 MB	16 MB	OK	CPU Bootflash size
2.1	2.1	OK	CPU hardware major.minor version
1.11	1.11	OK	CPU functional major.minor version

Linecard driver major.minor versions, (counts:Active=18, Standby=18)

Active CPU	Sby CPU	Sby Compat	Drv ID	Driver description
1.1	1.1	OK	0x1000	CPU w/o Switch Fabric
1.1	1.1	OK	0x1001	Fixed Transponder, w/monitor
1.1	1.1	OK	0x1002	Fixed Transponder, no monitor
1.1	1.1	OK	0x1003	Pluggable Transponder, w/monitor
1.1	1.1	OK	0x1004	Pluggable Transponder, no monitor
1.1	1.1	OK	0x1005	Line Card Motherboard
1.1	1.1	OK	0x1006	Backplane
Active CPU	Sby CPU	Sby Compat	Drv ID	Driver description
1.1	1.1	OK	0x1007	32-ch Mux/Demux
1.1	1.1	OK	0x1008	Fixed 4-ch Mux/Demux, no OSC
1.1	1.1	OK	0x1009	Fixed 8-ch Mux/Demux, no OSC
1.1	1.1	OK	0x100A	Modular 4-ch Mux/Demux, no OSC
1.1	1.1	OK	0x100B	Modular 8-ch Mux/Demux, no OSC
1.1	1.1	OK	0x100C	32-ch Array Wave Guide
1.1	1.1	OK	0x100D	Mux/Demux Motherboard
1.1	1.1	OK	0x100E	Modular 4-ch Mux/Demux plus OSC
1.1	1.1	OK	0x100F	Modular 8-ch Mux/Demux plus OSC
1.1	1.1	OK	0x1010	Mux-Demux Motherboard, no OSC
1.1	1.1	OK	0x1011	Line Card Motherboard, no splitter

Software sync client versions, listed as version range X-Y.

X indicates the oldest peer version it can communicate with.

Y indicates the current sync client version.

Sync client counts:Active=2, Standby=2

Active CPU	Sby CPU	Sby Compat	Cl ID	Redundancy Client description
ver 1-1	ver 1-1	OK	17	CPU Redundancy


```
ver 1-1 ver 1-1 OK 6 OIR Client
```

The following example shows how to display the running configuration file on the standby processor card:

```
sby-Switch# show redundancy running-config-file
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
no service dhcp
!
hostname Switch

<Information deleted>
```

Reloading the Processor Cards

To reload one or both of the processor cards, use the following privileged EXEC commands on the active processor card CLI:

Command	Purpose
redundancy reload peer	Reloads the standby processor card.
redundancy reload shelf	Reloads both processor cards in the shelf.

Example

The following example shows how to reload the standby processor card:

```
Switch# redundancy reload peer
Reload peer [confirm] y
Preparing to reload peer
```

Configuring Privileged EXEC Mode Access on the Standby Processor Card

Access to privileged EXEC mode from the standby processor card CLI can be enabled from the active processor card CLI. This feature provides extra security for the Cisco ONS 15540 ESPx system.

To configure access to privileged EXEC mode on the standby processor card, perform the following steps on the active processor card CLI, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# redundancy Switch(config-red)#	Enters redundancy configuration mode.
Step 2	Switch(config-red)# standby privilege-mode enable	Enables access to privileged EXEC mode from the standby processor card CLI. The default state is disabled.

Example

The following example shows how to configure redundancy maintenance mode:

```
Switch(config)# redundancy
Switch(config-red)# standby privilege-mode enable
```

Displaying the Standby Processor Card Privileged EXEC Mode Status

To display the privileged EXEC mode access status on the standby processor card, use the following privileged EXEC command:

Command	Purpose
<code>show redundancy summary</code>	Displays the redundancy configuration and status.

Example

The following example shows the privileged EXEC mode access status on the standby processor card:

```
Switch# show redundancy summary

Redundant system information
-----
Available Uptime:                2 days, 1 hour, 19 minutes
sysUpTime (switchover clears):  2 days, 1 hour, 19 minutes
Switchover Count:                0

Inter-CPU Communication State:  DOWN
Last Restart Reason:           Normal boot

Last Running Config sync:      never
Running Config sync status:    Out of Sync
Last Startup Config sync:      never
Startup Config sync status:    Out of Sync

This CPU is the Active CPU.
-----
Slot:                            6
Time since CPU Initialized:       2 days, 1 hour, 19 minutes
Image Version:                   ONS-15540 Software (ONS15540-I-M), Version 12.2
2)S1, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Image File:                       bootflash:ons15540-i-mz.122-22.S1
Software Redundancy State:        ACTIVE
Hardware State:                   ACTIVE
Hardware Severity:                0

Peer CPU is the Standby CPU.
-----
Slot:                            7
Time since CPU Initialized:       Unknown, peer CPU not responding
Image Version:                   Unknown, peer CPU not responding
Image File (on sby-CPU):         Unknown, peer CPU not responding
Software Redundancy State:        DISABLED
Hardware State:                   NON-PARTICIPANT
Hardware Severity:                2
Privilege Mode:                   Disabled

Switch#
```

About Preserving Counters on a Processor Card Switchover

The Cisco ONS 15540 ESPx supports line card traffic statistics and performance monitoring counters. The counters synchronize periodically from the primary processor card to the standby processor card enabling the system to preserve the statistics information across a processor card switchover. Traffic statistics and performance monitoring counters are preserved on the 2.5-Gbps transponder module and the 10-GE transponder module.

Table 3-4 lists the counters preserved over a processor card switchover.

Table 3-4 Counters Preserved Over a Processor Card Switchover

Card	Interface	Counters Supported
2.5-Gbps transponder module	Transparent (1-Gbps FC, 1-Gbps FICON, Gigabit Ethernet, ISC links compatibility mode traffic), encapsulation SONET/SDH	CVRD ¹ error count (8b10b)
		Section code violation error count
		Number of errored seconds
		Number of severely errored seconds
10-GE transponder module	tengigetheretnphy	CVRD error count(64b66b)
		10-GE non CDL packet count
		CDL HEC error count
		10-GE CDL idle packet count
	waveetheretnphy	CVRD error count(64b66b)
		10-GE non CDL packet count
		CDL HEC error count
		10-GE CDL idle packet count

1. CVRD = Code Violation and Running Disparity

Configuring Counter Preservation

To configure counter preservation on the processor card, perform the following steps on the active processor card CLI, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# redundancy Switch(config-red)#	Enters redundancy configuration mode.
Step 2	Switch(config-red)# auto-sync counters interface	Enables sync of interface counters.

Example

The following example shows how to enable or disable the preserving counters feature:

```
Switch (config)# redundancy
Switch (config-red)#auto-sync counters interface
```

Displaying the Counter Preservation Configuration

To display the counter preservation configuration on the processor card, use the following command:

Command	Purpose
<code>show redundancy capability</code>	Displays the processor card capabilities.

Example

The following example shows the counter preservation configuration on the processor card:

```
Switch#show redundancy capability
```

```
CPU capability support
```

Active CPU	Sby CPU	Sby Compat	CPU capability description
96 MB	0 MB	Unknown	CPU DRAM size
32 MB	0 MB	Unknown	CPU PMEM size
512 KB	0 KB	Unknown	CPU NVRAM size
16 MB	0 MB	Unknown	CPU Bootflash size
6.5	0.0	Unknown	CPU hardware major.minor version
1.25	0.0	Unknown	CPU functional major.minor version

```
Linecard driver major.minor versions, (counts: Active=43, Standby=0)
```

Active CPU	Sby CPU	Sby Compat	Drv/Ch/F ID	Driver description
1.1		Unknown	0x1000/0/0	CPU w/o Switch Fabric
1.1		Unknown	0x1001/1/0	Fixed Transponder, w/monitor
1.1		Unknown	0x1002/0/0	Fixed Transponder, no monitor
1.1		Unknown	0x1003/1/0	Pluggable Transponder, w/moni
1.1		Unknown	0x1004/0/0	Pluggable Transponder, no mon
2.1		Unknown	0x1005/0/0	Line Card Motherboard
1.1		Unknown	0x1006/0/0	Backplane
1.1		Unknown	0x1007/0/0	32-ch Mux/Demux
Active CPU	Sby CPU	Sby Compat	Drv/Ch/F ID	Driver description
1.1		Unknown	0x1008/0/0	Fixed 4-ch Mux/Demux, no OSC
1.1		Unknown	0x1009/0/0	Fixed 8-ch Mux/Demux, no OSC
1.1		Unknown	0x100A/0/0	Modular 4-ch Mux/Demux, no OS
1.1		Unknown	0x100B/0/0	Modular 8-ch Mux/Demux, no OS
1.1		Unknown	0x100C/0/0	32-ch Array Wave Guide
2.1		Unknown	0x100D/0/0	Mux/Demux Motherboard
1.1		Unknown	0x100E/0/0	Modular 4-ch Mux/Demux plus O
1.1		Unknown	0x100F/0/0	Modular 8-ch Mux/Demux plus O
2.1		Unknown	0x1010/0/0	Mux-Demux Motherboard, no OSC
2.1		Unknown	0x1011/0/0	Line Card Motherboard, no pro
3.1		Unknown	0x1012/0/0	Down Link Motherboard
1.1		Unknown	0x1013/0/0	OC192 Down Link DaughterCard
2.1		Unknown	0x1014/1/0	10G Down Link DaughterCard
1.1		Unknown	0x1015/0/0	Modular 16-ch Mux/Demux, no O
1.1		Unknown	0x1016/0/0	Modular 16-ch Mux/Demux plus
2.1		Unknown	0x1017/0/0	Line Card Motherboard, no pro
1.1		Unknown	0x1018/1/0	Low bit rate Type-1 transpond
2.1		Unknown	0x1019/0/0	CN Tower Line Card Motherboar
2.1		Unknown	0x101A/0/0	Mux/Demux Motherboard
1.1		Unknown	0x101B/0/0	Modular 4-ch Mux/Demux no OSC

1.1		Unknown	0x101C/0/0	Modular 4-ch Mux/Demux plus 0
1.1		Unknown	0x101D/0/0	Modular 8-ch Mux/Demux no OSC
1.1		Unknown	0x101E/0/0	Modular 8-ch Mux/Demux plus 0
Active CPU	Sby CPU	Sby Compat	Drv/Ch/F ID	Driver description

1.1		Unknown	0x101F/0/0	32-ch Array Wave Guide
2.1		Unknown	0x1020/0/0	Mux/Demux Motherboard, no OSC
1.1		Unknown	0x1021/0/0	POM Adapter
2.1		Unknown	0x1022/0/0	Down Link Motherboard, no pro
2.1		Unknown	0x1023/0/0	Down Link Motherboard, no pro
2.1		Unknown	0x1024/0/0	Line Card Motherboard, no pro
1.1		Unknown	0x1025/0/0	Modular 16-ch Mux/Demux, no 0
1.1		Unknown	0x1026/0/0	Modular 16-ch Mux/Demux plus
1.1		Unknown	0x1027/0/0	PSM Trunk switch protection
1.1		Unknown	0x1028/1/0	non-plug type1 xpdr with con
1.1		Unknown	0x1029/1/0	Low bit rate type-1 xpdr w/co
1.1		Unknown	0x1000/0/1	ONS15540 Rommon

Software sync client versions, listed as version range X-Y.
 X indicates the oldest peer version it can communicate with.
 Y indicates the current sync client version.
 Sync client counts: Active=6, Standby=0

Active CPU	Sby CPU	Sby Compat	Cl ID	Redundancy Client description

ver 1-2		Unknown	17	CPU Redundancy
ver 1-1		Unknown	19	Interface Sync
ver 1-1		Unknown	36	MetOpt Password Sync
Active CPU	Sby CPU	Sby Compat	Cl ID	Redundancy Client description

ver 1-2		Unknown	18	Online Diagnostics
ver 1-2		Unknown	6	OIR Client
ver 1-1		Unknown	27	metopt cm db sync

Local backplane IDPROM	
Backplane IDPROM field	Local CPU

idversion	1
magic	153
card_type	4102
order_part_num_str	15540-CHSA
description_str	CN_Tower_Backplane
board_part_num_str	73-5655-03
board_revision_str	02
serial_number_str	TBC04501952
date_of_manufacture_str	01/09/2002
deviation_numbers_str	0
manufacturing_use	0
rma_number_str	0x00
rma_failure_code_str	0x00
oem_str	Cisco_Systems
clei_str	
Backplane IDPROM field	Local CPU

snmp_oid_substr	0
schematic_num_str	92-4113-03
hardware_major_version	3
hardware_minor_version	0
engineering_use_str	1
crc16	47732
user_track_string	lab
diagst	^A
board_specific_revision	1

```

board_specific_magic_number    153
board_specific_length          57
mac_address_block_size        16
mac_address_base_str           000016443eb70
cpu_number                     0
optical_backplane_type        2
Switch#

```

About the Software Configuration Register

The Cisco ONS 15540 ESPx uses a 16-bit software configuration register to set specific system parameters. Settings for the software configuration register are written into NVRAM (nonvolatile random access memory).

You can change the software configuration register settings for the following reasons:

- Force the system into the ROM monitor or boot ROM
- Select a boot source and default boot filename
- Enable or disable the break function
- Control broadcast addresses
- Set the console terminal baud rate
- Load operating software from Flash memory
- Enable booting from a TFTP server
- Recover a lost password
- Boot the system manually using the **boot** command at the bootstrap program prompt.
- Force the system to boot automatically from the system bootstrap software (boot image) or from its default system image in onboard Flash memory, using any **boot system** commands stored in the startup configuration file in NVRAM

Software Configuration Register Settings

Table 3-5 describes each of the software configuration register bits.



Caution

To avoid confusion and possibly halting the system, remember that valid configuration register settings might be combinations of settings and not just the individual settings listed in Table 3-5. For example, the value of 0x0101 is a combination of settings (bit 8 is 0x0100 and bits 00 through 03 are 0x0001).

Table 3-5 Software Configuration Register Bits

Bit Number	Hexadecimal	Description
00 to 03	0x0000 to 0x000F	Controls the system boot behavior (also known as the boot field)
06	0x0040	Causes system software to ignore NVRAM contents
07	0x0080	Enables the OEM bit
08	0x0100	Disables the break function
09	0x0200	Uses secondary bootstrap during system boot

Table 3-5 Software Configuration Register Bits (continued)

Bit Number	Hexadecimal	Description
10	0x0400	Uses an IP broadcast with all zeros
11 to 12	0x0800 to 0x1000	Sets the console line speed (default is 9600 baud)
13	0x2000	Boots the default Flash software if network boot fails
14	0x4000	Uses IP broadcasts without network numbers
15	0x8000	Enables diagnostic messages and ignores the NVRAM contents

Bit 8 controls the console break function. Setting bit 8 (the factory default) causes the system to ignore the console break key. Clearing bit 8 cause the system to use the break key or break signal as a command to force the system into the bootstrap monitor (ROMMON), thereby halting normal operation. Regardless of the setting of the break enable bit, a break causes a return to the ROMMON during the first few seconds (approximately five seconds) of booting.

Bit 9 controls the secondary bootstrap program function. Setting bit 9 causes the system to use the secondary bootstrap. Clearing bit 9 (the factory default) causes the system to ignore the secondary bootstrap. The secondary bootstrap program is used for system debugging and diagnostics.

Bit 10 controls the host portion of the IP broadcast address. Setting bit 10 causes the system to use all zeros. Clearing bit 10 (the factory default) causes the system to use all ones. Bit 10 interacts with bit 14, which controls the network and subnet portions of the IP broadcast address.

Table 3-6 shows the combined effect of bits 14 and 10.

Table 3-6 Register Settings for Broadcast Address

Bit 14	Bit 10	Address (<net><host>)
0	0	<ones><ones>
0	1	<ones><zeros>
1	0	<net><ones>
1	1	<net><zeros>

Bit 12 and bit 11 in the configuration register determine the data transmission rate of the console terminal. Table 3-7 shows the bit settings for the four available rates. The factory-set default data transmission rate is 9600.

Table 3-7 Settings for Console Terminal Transmission Rate

Bit 12	Bit 11	Baud Rate
0	0	9600
0	1	4800
1	0	1200
1	1	2400

Bit 13 determines the system response to a bootload failure. Setting bit 13 (the factory default) causes the system to load operating software from bootflash memory after five unsuccessful attempts to load a boot file from the Flash memory device in slot 0. Clearing bit 13 causes the server to continue attempting to load a boot file from bootflash indefinitely.

Boot Field Values

The lowest four bits of the configuration register (bits 3, 2, 1, and 0) form the boot field. The order in which the system looks for system bootstrap information depends on the boot field setting in the configuration register.

Table 3-8 describes the values for the boot field.

Table 3-8 Configuration Register Boot Field Values

Boot Field Value	Description
0x0 (0-0-0-0)	Stays at the system bootstrap prompt. You must boot the operating system manually by giving a boot command to the ROMMON system bootstrap environment.
0x1 (0-0-0-1)	Boots the first system image in onboard Flash SIMM. If the boot fails, the system stops booting and remains in ROMMON mode.
0x2 (0-0-1-0) to 0xF (1-1-1-1)	Loads the system image specified by boot system commands in the startup configuration file. When the startup configuration file does not contain boot system commands, the system tries to load the first system image stored on the Flash memory device in slot 0. If that attempt fails, the system tries to boot with the first system image in bootflash. If that also fails, the system stops booting and remains in ROMMON mode. The factory default is 0x2.

Default System Boot Behavior

The factory default value for the configuration register on the Cisco ONS 15540 ESPx is 0x2102. When the system boots, the following occurs:

- The system attempts to load the system images specified in the **boot system** commands in the startup configuration file. If no **boot system** commands are configured, the system attempts to load the first system image stored on the Flash memory device in slot 0.
- The console Break key sequence, or break signal, is disabled and the system ignores it while rebooting.



Note Regardless of the setting of the break enable bit, a break causes a return to the ROMMON during the first few seconds (approximately five seconds) of booting.

- After five failed attempts to load a system image on the Flash memory device in slot 0, the system loads the first system image from Flash memory. If that attempt fails, the system stays in ROMMON mode.

Boot Command

You can enter only the **boot** command, or you can include additional boot instructions, such as the name of a file stored in Flash memory or a file that you specify for booting from a network server.

If you use the **boot** command without specifying a file or any other boot instructions, the system boots using the default system image (the first system image in onboard Flash memory). Otherwise, you can instruct the system to boot from a specific system image in Flash memory (using the **boot filename** command) or by sending a direct TFTP request to a specific server (using the **boot filename ip-address** command).

For more information on system booting, see refer to the *Cisco ONS 15540 ESPx Software Upgrade Guide*.

Changing the Software Configuration Register

To change the configuration register, perform the following steps:

	Command	Purpose
Step 1	Switch# configure terminal Switch(config)#	Enters global configuration mode.
Step 2	Switch(config)# config-register <i>value</i>	Sets the contents of the configuration register. The <i>value</i> is a hexadecimal number preceded by 0x . See Table 3-5 for the list of values. Note The new configuration register value takes effect at the next system reload.
Step 3	Switch(config)# end Switch#	Returns to privileged EXEC mode.
Step 4	Switch# reload	(Optional) Reloads the system using the new configuration register value.



Note The factory default value for the register is 0x2102.

Example

The following example shows how to configure the system to manually boot from the ROMMON prompt:

```
Switch# configuration terminal
Switch(config)# config-register 0x100
Switch(config)# end
Switch# reload
```

Verify the Configuration Register Value

To verify the configuration register value, use the following EXEC command:

Command	Purpose
Switch# show version	Displays the current configuration register value. This value is used at the next system reload.

Example

The following example shows how to configure the system to examine the startup configuration file for boot system options:

```
Switch# show version
```

```
<Information deleted>
```

```
Configuration register is 0x2102 (will be 0x100 at next reload)
```

About Fan Failure Shutdown

The Cisco ONS 15540 ESPx fan assembly is located at the bottom of the chassis and contains eight individual fans and a fan controller board. The controller board monitors the status of each fan and reports the status to the processor card.

If a single fan fails, a minor alarm is reported to the processor card. However, the chassis will never reach critical high temperature when only one fan fails.

If two or more fans fail, a major alarm is reported to the processor card.

If all eight fans in the fan tray fail, the chassis will reach critical temperature after 14 minutes.

To prevent damage to the cards and modules in the shelf when two or more fans fail, you can configure the system to automatically power off the following components:

- 2.5-Gbps transponder modules
- 10-GE transponder modules



Note

The 2.5-Gbps transponder modules power off if the hardware version of the 2.5-Gbps line card motherboard is 2.1 or later; otherwise, the 2.5-Gbps transponder modules reset. Use the **show hardware** command to determine the hardware version of the 2.5-Gbps line card motherboards.

To recover from fan failure shutdown, you must power-cycle the shelf.



Caution

Do not save the startup configuration file after the line modules shutdown. This action would result in losing the previous startup configuration.



Caution

The fan failure shutdown feature disrupts traffic on the shelf when two or more fans fail.

Configuring Fan Failure Shutdown

To configure the system to automatically shut down when two or more fans fail, use the following global configuration command:

Command	Purpose
<code>environment-monitor shutdown fan</code>	Enables fan tray failure shutdown.



Note

The system will start powering off or resetting the transponder modules about 2 minutes after detecting that two or more fans have failed.

Example

The following example shows how to enable fan tray failure shutdown:

```
Switch(config)# environment-monitor shutdown fan
```

Displaying the Fan Tray Failure Shutdown Configuration

To display the fan tray failure shutdown configuration, use the following EXEC command:

Command	Purpose
<code>show environment</code>	Displays the fan tray failure shutdown configuration.

Example

The following example shows how to display the fan tray failure shutdown feature configuration:

```
Switch# show environment
```

```
Fan
```

```
---
```

```
Status:                Total Failure
```

→ Line card shutdown on fan failure:enabled

```

      Sensor                Temperature          Thresholds
                        (degree C)      Minor      Major      Critical      Low
-----
Inlet Sensor             28           65         75         80         -15
Outlet Sensor            28           75         85         90         -15

```

```

      Sensor                Alarms
                        Min
-----
Critical
-----
Inlet Sensor             0           0           0
Outlet Sensor            0           0           0

```

```
Power Entry Module 0 type DC status:      OK
```

About Critical Temperature Shutdown

Cisco ONS 15540 ESPx utilizes the temperature sensors on its CPU switch module to detect abnormal temperature conditions during system operation. Thermal monitoring of chassis components provides early warning indications of possible component failure to ensure safe and reliable system operation and avoid network interruptions. A temperature sensor might trip in response to elevated ambient air temperature, a clogged air filter or other airflow blockage, or a combination of these causes.

The Cisco ONS 15540 ESPx system generates four types of alarms: critical, major, minor, and low. The following table provides the default threshold temperatures for these alarms:

Alarm	Air Inlet Sensor Threshold Temperature in degree Celsius (° C)	Air Outlet Sensor Threshold Temperature in degree Celsius (° C)
Minor	50	55
Major	60	65
Critical	70	75
Low	-15	-15



Note

You can override the default threshold temperatures by issuing the **environment-monitor temperature-threshold** command in the global configuration mode.

The Cisco ONS 15540 ESPx system automatically resets the following cards if the operating temperature exceeds the critical threshold:

- ESCON aggregation cards
- 8-port FC/GE aggregations cards
- 2.5-Gbps ITU trunk cards
- 10-Gbps ITU trunk cards
- Transponder line cards
- Multirate cards

All the other cards will be shutdown if the operating temperature exceeds the critical threshold. In addition, the ITU lasers on the trunk cards will be powered off. Though possible, Cisco does not recommend that you disable this feature.

To recover from a shutdown, you must power-cycle the shelf.



Caution

Do not save the startup configuration file after the line cards shut down. This action would result in losing the previous startup configuration.



Caution

The shutdown feature disrupts traffic on the shelf when the operating temperature exceeds the critical temperature.

Configuring Critical Temperature Shutdown

To configure the system to automatically shut down when a critical alarm is generated, use the following global configuration command:

Command	Purpose
environment-monitor shutdown temperature <i>slot/subslot/module</i>	Enables system shutdown if the operating temperature exceeds the critical threshold temperature.

To change the default threshold temperatures, use the following global configuration command:

Command	Purpose
environment-monitor temperature-threshold {critical major minor low} <i>slot/subslot/module</i> <threshold value>	Sets new ¹ threshold temperatures for the specified module.

1. If you do not specify the threshold temperature for an alarm (critical, major, minor, or low), the threshold will be reset to the default value. If you do not specify the module as well, the threshold temperature will be reset for all the modules.

To reset all thresholds for all modules, use the following global configuration command:

Command	Purpose
no environment-monitor temperature-threshold	Resets all thresholds to the default temperatures for all modules.

Example

The following example shows how to configure the critical threshold temperature:

```
Switch(config)# environment-monitor temperature-threshold critical 6/0/0 65
```

Displaying the Threshold Temperatures

To display the configured threshold temperatures, use the following EXEC command:

Command	Purpose
show environment	Displays the configured threshold temperatures.

Example

The following example shows how to display the configured threshold temperatures:

```
Switch# show environment
Fan
---
Status:                Total Failure

Line card shutdown on fan failure: disabled
```

Sensor	Module	Temperature (degree C)	Thresholds			
			Minor	Major	Critical	Low
→ Inlet Sensor	6/0/0	29	35	45	65	-5
Outlet Sensor	6/0/1	30	40	50	65	-15

Sensor	Module	Version	Alarms			Shutdown Mode
			Minor	Major	Critical	
Inlet Sensor	6/0/0	A	0	0	0	Chassis
Outlet Sensor	6/0/1	A	0	0	0	Chassis

Power Entry Module 1 type DC status: OK



Configuring 2.5-Gbps Transponder Module Interfaces and Patch Connections

This chapter describes how to configure interfaces and patch connections on the Cisco ONS 15540 ESPx. This chapter includes the following sections:

- Configuring Protocol Encapsulation or Clock Rate, page 4-2
- About Protocol Monitoring, page 4-6
- Configuring Protocol Monitoring, page 4-8
- About Alarm Thresholds, page 4-9
- Configuring Alarm Thresholds, page 4-9
- About Laser Shutdown, page 4-13
- Configuring Laser Shutdown, page 4-16
- Configuring Transponder Channel Frequency, page 4-18
- Configuring Optical Power Thresholds, page 4-19
- About Patch Connections, page 4-21
- Configuring Patch Connections, page 4-21
- About Cross Connections, page 4-24
- About Performance History Counters, page 4-25
- Displaying Performance History Counters, page 4-26



Note

To ensure the installed Cisco IOS software supports your hardware and provides the software features you wish to use, see the “New and Changed Information” section on page xviii. Also refer to the “Hardware Supported” section and “Feature Set” section of the latest release notes for the Cisco ONS 15540 ESPx.

To configure transparent interfaces on the Cisco ONS 15540 ESPx, perform the following steps:

- Step 1** Specify the protocol encapsulation and, if required, the transmission rate and OFC (open fiber control), or specify the signal clock rate (required).
- Step 2** Enable protocol monitoring (optional).
- Step 3** Create alarm threshold lists and apply them to the interfaces (optional).

Step 4 Enable forward laser control (optional).

To configure wave interfaces on the Cisco ONS 15540 ESPx, perform the following steps:

Step 1 Enable forward laser control (optional).

Step 2 Enable laser safety protocol (optional).

To configure patch connections on the Cisco ONS 15540 ESPx, perform the following steps:

Step 1 Configure the patch connections (required).

Step 2 Configure the patch connections between the OSC (optical supervisory channel) interface on the mux/demux motherboards and the mux/demux modules (required if the OSC is present).

Configuring Protocol Encapsulation or Clock Rate

A transparent interface does not terminate the protocol of the signal it receives but it does convert it from an optical signal to an electrical signal and back to an optical signal. Therefore, you must configure the signal transmission rate by specifying either the protocol encapsulation or the clock rate.

To configure the protocol encapsulation or the clock rate for a transparent interface, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface transparent <i>slot/subcard/0</i> Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# encapsulation {fastethernet fddi gigabitethernet escon} or Switch(config-if)# encapsulation sysplex clo or Switch(config-if)# encapsulation sysplex etr or Switch(config-if)# encapsulation sysplex isc {compatibility peer [1g 2g]} or Switch(config-if)# encapsulation ficon {1g 2g} or Switch(config-if)# encapsulation sonet {oc3 oc12 oc48} or Switch(config-if)# encapsulation sdh {stm-1 stm-4 stm-16} or Switch(config-if)# encapsulation fibrechannel {1g 2g} [ofc {enable disable}] or Switch(config-if)# clock rate value	Specifies Fast Ethernet, FDDI, Gigabit Ethernet, or ESCON. OFC ¹ is disabled. Specifies Sysplex CLO ² . OFC is disabled. Forward laser control is enabled on both the transparent and wave interfaces. OFC is disabled. Specifies Sysplex ETR ³ . OFC is disabled. Specifies ISC ⁴ compatibility mode (1 Gbps) or peer mode (1 Gbps or 2 Gbps). OFC is enabled for compatibility mode CSCDV42166 and disabled for peer mode. Specifies FICON as the signal protocol and 1 Gbps or 2 Gbps as the transmission rate. OFC is disabled. Specifies SONET as the signal protocol and OC-3, OC-12, or OC-48 as the transmission rate. OFC is disabled. Specifies SDH as the signal protocol and STM-1, STM-4, or STM-16 as the transmission rate. OFC is disabled. Specifies Fibre Channel as the signal protocol and 1 Gbps or 2 Gbps as the transmission rate. Enables or disables OFC. OFC is disabled by default. Specifies the signal transmission clock rate without an associated protocol. OFC is disabled. Note Protocol monitoring cannot be enabled on the interface when the clock rate command is configured.

1. For information about OFC, see the "About Laser Shutdown" section on page 4-13.
2. CLO = control link oscillator
3. ETR = external timer reference
4. ISC = Intersystem Channel Links

**Note**

Disable autonegotiation 2-Gbps Fibre Channel client equipment connected to Cisco ONS 15540 ESPx and set the speed to match the clock rate or protocol encapsulation set on the transparent interfaces. The transponder modules only recognize the configured clock rate or protocol encapsulation and do not support autonegotiation.

**Caution**

Do not configure y-cable protection with Sysplex CLO, Sysplex ETR, or ISC compatibility protocol encapsulation, or with the OFC safety protocol.

**Note**

Sysplex CLO and Sysplex ETR are supported outside the nominal range of the clock rates for the Cisco ONS 15540 ESPx because of the nature of the traffic type.

Table 4-1 lists the clock rates for well-known protocols supported by the 2.5-Gbps transponder module:

Table 4-1 Supported Clock Rates for Well-Known Protocols

Well-Known Protocol	Clock Rate (in kbps)
DS3	44,736
DV1 ¹ in ADI ² mode	270,000
E3	34,368
ESCON	200,000
Fibre Channel (1 Gbps)	1,062,500
Fibre Channel (2 Gbps)	2,125,000
FICON (1 Gbps)	1,062,500
FICON (2 Gbps)	2,125,000
Gigabit Ethernet	1,250,000
ISC Compatibility Mode (ISC-1)	1,062,500
ISC Peer Mode (ISC-3)	2,125,000
SONET OC-1	51,840
SONET OC-3/SDH STM-1	155,520
SONET OC-12/SDH STM-4	622,080
SONET OC-24/SDH STM-8	933,120
SONET OC-48SDH STM-16	2,488,320

1. DV = digital video
2. ADI = Asynchronous Digital Interface

**Note**

Data coding, as well as clock rate, determines whether a particular traffic type is supported on Cisco ONS 15540 ESPx transponder modules. For information on supported traffic types, contact your SE (systems engineer) at Cisco Systems.

**Note**

Error-free transmission of some D1 video signals (defined by the SMPTE 259M standard) and test patterns (such as Matrix SDI) cannot be guaranteed by the Cisco ONS 15500 Series because of the pathological pattern in D1 video. This well-known limitation is usually overcome by the D1 video equipment vendor, who uses a proprietary, second level of scrambling. No standards exist at this time for the second level of scrambling.

The following ranges are not supported by the SM transponder module hardware and the MM transponder module hardware:

- 851,000 kbps to 999,999 kbps
- 1,601,000 kbps to 1,999,999 kbps

For clock rate values outside of these unsupported ranges and not listed in Table 4-1, contact your SE (systems engineer) at Cisco Systems.

**Note**

Use the encapsulation command for clock rates supported by protocol monitoring rather than the clock rate command. For more information protocol monitoring, see the “About Protocol Monitoring” section on page 4-6.

**Caution**

The SFP optics supported by the extended range transponder modules yield optimal performance at the data rates for which the SFP optics are explicitly designed. Configuring a protocol encapsulation or clock rate outside of the clock rate specifications for the SFP optics could result in suboptimal performance, depending on the SFP optics characteristics (such as receiver sensitivity and output power).

For information on SFP optics specifications, refer to the *Cisco ONS 15540 ESPx Hardware Installation Guide*.

**Note**

When you must use Sysplex CLO encapsulation or Sysplex ETR encapsulation, you must configure APS bidirectional path switching. For more information on APS and bidirectional path switching, see Chapter 7, “Configuring APS.”

Examples

The following example shows how to configure GE (Gigabit Ethernet) encapsulation on a transparent interface:

```
Switch(config)# interface transparent 8/0/0
Switch(config-if)# encapsulation gigabitethernet
```

The following example shows how to configure a clock rate on a transparent interface:

```
Switch(config)# interface transparent 10/1/0
Switch(config-if)# clock rate 1065
```

**Note**

Removing the protocol encapsulation or the clock rate does not shut down the transmit lasers. To shut down the lasers, use the **shutdown** command.

Displaying Protocol Encapsulation or Clock Rate Configuration

To display the protocol encapsulation configuration of a transparent interface, use the following EXEC command:

Command	Purpose
show interfaces transparent <i>slot/subcard/0</i>	Displays the transparent interface configuration.

Examples

The following example shows how to display the protocol encapsulation configuration of a transparent interface:

```
Switch# show interfaces transparent 8/0/0
Transparent11/3/0 is up, line protocol is up
  Encapsulation: GigabitEthernet
  Signal monitoring: off
  Time of last "monitor" state change never
  Time of last "encapsulation" change 00:00:03
  Forward laser control: Off
  Configured threshold Group: None
  Loopback not set
  Last clearing of "show interface" counters 00:00:03
  Hardware is transparent
```

The following example shows how to display the clock rate configuration of a transparent interface:

```
Switch# show interfaces transparent 10/1/0
Transparent11/3/0 is up, line protocol is up
  Encapsulation: Unknown
  Clock rate: 1000000 KHz
  Signal monitoring: off
  Time of last "monitor" state change never
  Time of last "encapsulation" change never
  Forward laser control: Off
  Configured threshold Group: None
  Loopback not set
  Last clearing of "show interface" counters never
  Hardware is transparent
```

About Protocol Monitoring

Transparent interfaces on the Cisco ONS 15540 ESPx can be configured to monitor protocol and signal performance. When monitoring is enabled, the system maintains statistics that are used to determine the quality of the signal.

The following protocols can be monitored:

- ESCON (Enterprise Systems Connection)
- Fibre Channel (1 Gbps and 2 Gbps)
- FICON (Fiber Connection) (1 Gbps and 2 Gbps)
- Gigabit Ethernet
- ISC (InterSystem Channel) links compatibility mode
- ISC links peer mode(1-Gbps and 2-Gbps)
- SDH (Synchronous Digital Hierarchy) (STM-1, STM-4, STM-16)

- SONET (OC-3, OC-12, OC-48)

**Note**

Enabling monitoring on a transparent interface also enables monitoring on the corresponding wave interface. For example, if you enable monitoring on transparent interface 3/0/0, monitoring is also enabled on wave interface 3/0.

**Note**

To monitor 2-Gbps FC, FICON, and ISC links peer mode, you must upgrade the transponder module functional image to release 1.A3. For information on upgrading functional images, refer to the *Cisco ONS 15540 ESPx Software Upgrade Guide*.

For GE, FC, and FICON traffic, the Cisco ONS 15540 ESPx monitors the following conditions:

- CVRD (code violation running disparity) error counts
- Loss of Sync
- Loss of Lock
- Loss of Light

For SONET errors, the Cisco ONS 15540 ESPx monitors the SONET section overhead only, not the SONET line overhead. Specifically, the Cisco ONS 15540 ESPx monitors the B1 byte and the framing bytes. The system can detect the following defect conditions:

- Loss of light
- Loss of lock (when the clock cannot be recovered from the received data stream)
- Severely errored frame
- Loss of frame

For SONET performance, the system monitors the B1 byte, which is used to compute the four SONET section layer performance monitor parameters:

The definitions for these acronyms come from the Telcordia SONET standard spec page 6-110.

- SEFS-S (second severely errored framing seconds)
- CV-S (section code violations)
- ES-S (section errored seconds)
- SES-S (section severely errored seconds)

For ISC traffic, the system monitors the following conditions:

- CVRD error counts
- Loss of CDR (clock data recovery) Lock
- Loss of Light

Configuring Protocol Monitoring

To configure protocol monitoring on a transparent interface, and its corresponding wave interface, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface transparent slot/subcard/0 Switch(config-if)#	Selects the transparent interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# monitor enable	Enables signal monitoring. Note Protocol encapsulation must be configured on the transparent interface before enabling monitoring.

Examples

The following example shows how to enable protocol monitoring on a transparent interface:

```
Switch(config)# interface transparent 10/0/0
Switch(config-if)# monitor enable
```

The following example shows how to disable protocol monitoring on a transparent interface:

```
Switch(config)# interface transparent 10/0/0
Switch(config-if)# no monitor enable
```

Displaying Protocol Monitoring Configuration

To display the protocol monitoring configuration of a transparent interface, use the following EXEC command:

Command	Purpose
show interfaces {transparent slot/subcard/0 wave slot/subcard}	Displays the transparent interface configuration.

Examples

The following example shows how to display the protocol monitoring configuration of a transparent interface:

```
Switch# show interfaces transparent 10/0/0
Transparent10/0/0 is up, line protocol is up
  Signal quality: Signal degrade threshold exceeded
  Encapsulation: Sonet   Rate: oc3
  Signal monitoring: on
  Forward laser control: Off
  Configured threshold Group: None
  Section code violation error count(bip1): 3714369135
  Number of errored seconds(es): 57209
  Number of severely errored seconds(ses): 57209
  Number of severely errored framing seconds(sefs): 0
  Number of times SEF alarm raised: 0
  Number of times SF threshold exceeded: 0
  Number of times SD threshold exceeded: 384
  Loopback not set
  Last clearing of "show interface" counters never
```

Hardware is transparent

The following example shows how to display the protocol monitoring configuration of a wave interface:

```
Switch# show interfaces wave 10/0
Wave10/0 is up, line protocol is up
  Channel: 25   Frequency: 195.1 Thz   Wavelength: 1536.61 nm
  Splitter Protected: No
  Receiver power level: -7.0 dBm
  Laser safety control: Off
  Forward laser control: Off
  Osc physical port: No
  Wavelength used for inband management: No
  Configured threshold Group: None
  Section code violation error count(bip1): 929326
  Number of errored seconds(es): 30
  Number of severely errored seconds(ses): 30
  Number of severely errored framing seconds(sefs): 0
  Number of times SEF alarm raised: 0
  Number of times SF threshold exceeded: 0
  Number of times SD threshold exceeded: 0
  Loopback not set
  Last clearing of "show interface" counters never
  Hardware is data_only_port
```

About Alarm Thresholds

You can configure thresholds on transparent and wave interfaces that issue alarm messages to the system if the thresholds are exceeded. The threshold values are applied to both transparent and wave interfaces on a transponder module when protocol monitoring is enabled on the transparent interface.

The rate is based on the protocol encapsulation or the clock rate for the interface. Every second, the monitoring facility updates the counters that correspond to the alarm thresholds. When the signal degrades, or fails entirely, the system issues alarms to the console. These alarms can help isolate failures in the system and in the network.

You can configure more than one threshold list on an interface. The threshold lists cannot have overlapping counters so that only one counter is set for the interface. Also, the threshold list name cannot begin with the text string “default” because the it is reserved for use by the system.

Configuring Alarm Thresholds

To configure alarm thresholds on transparent interfaces, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# threshold-list <i>name</i> Switch(config-t-list)#	Creates or selects the threshold list to configure and enters threshold list configuration mode. Note You cannot modify an existing threshold list if it is associated with an interface.
Step 2	Switch(config-t-list)# notification-throttle timer <i>seconds</i>	Configures the SNMP notification timer. The default value is 5 seconds. (Optional)

	Command	Purpose
Step 3	Switch(config-t-list)# threshold name {cvrd cdl hec crc sonet-sdh section cv tx-crc} {failure degrade} [index value] Switch(config-threshold)#	Specifies a threshold type to modify and enters threshold configuration mode.
Step 4	Switch(config-threshold)# value rate value	Specifies the threshold rate value. This value is the negative power of 10 (10 ⁻ⁿ).
Step 5	Switch(config-threshold)# description text	Specifies a description of the threshold. The default value is the null string. (Optional)
Step 6	Switch(config-threshold)# aps trigger	Enables APS switchover when this threshold is crossed. (Optional) Note This command only triggers switchovers for y-cable protection, not for splitter protection.
Step 7	Switch(config-threshold)# exit Switch(config-t-list)#	Returns to threshold list configuration mode. Repeat Step 3 through Step 7 to configure more thresholds in the threshold list.
Step 8	Switch(config-t-list)# exit Switch(config)#	Returns to global configuration mode.
Step 9	Switch(config)# interface {transparent slot/subcard/0 wave slot/subcard} Switch(config-if)#	Selects the transparent or wave interface to configure and enters interface configuration mode.
Step 10	Switch(config-if)# threshold-group name	Configures the threshold list on the interface.

**Note**

If a threshold type does not apply to the encapsulation type for the interface, that threshold type is ignored.

**Note**

For y-cable protected transparent and wave interfaces, disable monitoring on the interface with the **no monitor** command before removing an alarm threshold. Use the **show aps** command to determine the protection configuration for the interface.

Table 4-3 lists the threshold error rates in errors per second for each of the protocol encapsulations.

Table 4-2 Threshold Error Rates for Monitored Protocols in Errors Per Second

Rate	SONET OC-3 or SDH STM-1	SONET OC-12 or SDH STM-4	SONET OC-48 or SDH STM-16	Gigabit Ethernet	ESCON	FICON	Fibre Channel ¹
3	31753	32000	32000	1244390	199102	1057731	1057731
4	12318	27421	31987	124944	19991	106202	106202
5	1518	5654	17296	12499	2000	10625	10625
6	155	616	2394	1250	200	1062	1062
7	15.5	62	248	125	20	106	106

Table 4-2 Threshold Error Rates for Monitored Protocols in Errors Per Second

Rate	SONET OC-3 or SDH STM-1	SONET OC-12 or SDH STM-4	SONET OC-48 or SDH STM-16	Gigabit Ethernet	ESCON	FICON	Fibre Channel ¹
8	1.55	6.2	24.8	12.5	2	10.6	10.6
9	0.155	0.62	2.48	1.25	0.2	1.06	1.06

1. Only the 1 Gbps rate is monitored.

Table 4-3 Thresholds for Monitored Protocols (Errors Per Second)

Rate	SONET OC-3 or SDH STM-1	SONET OC-12 or SDH STM-4	SONET OC-48 or SDH STM-16	Gigabit Ethernet	ESCON	FICON	Fibre Channel ¹	ISC ²
3	31,753 ³	32,000 ³	32,000 ³	1,244,390	199,102	1,057,731	1,057,731	1,057,731
4	12,318	27,421	31,987 ³	124,944	19,991	106,202	106,202	106,202
5	1518	5654	17,296	12,499	2000	10,625	10,625	10,625
6	155	616	2394	1250	200	1062	1062	1062
7	15.5	62	248	125	20	106	106	106
8	1.55	6.2	24.8	12.5	2	10.6	10.6	10.6
9	0.155	0.62	2.48	1.25	0.2	1.06	1.06	1.06

1. One Gbps rate only.

2. Compatibility mode only.

3. Rate is limited by the hardware.

Examples

The following example shows how to create an alarm threshold list and configure that list on a transparent interface:

```
Switch# configure terminal
Switch(config)# threshold-list sonet-counters
Switch(config-t-list)# threshold name sonet-sdh section cv degrade
Switch(config-threshold)# value rate 9
Switch(config-threshold)# exit
Switch(config-t-list)# threshold name sonet-sdh section cv failure
Switch(config-threshold)# value rate 7
Switch(config-threshold)# exit
Switch(config-t-list)# exit
Switch(config)# interface transparent 10/0/0
Switch(config-if)# threshold-group sonet-counters
```

The following example shows how to create an alarm threshold list with the APS switchover trigger and configure that list on a pair of associated transparent interfaces:

```
Switch(config)# threshold-list sonet-alarms
Switch(config-t-list)# threshold name sonet-sdh section cv failure
Switch(config-threshold)# value rate 6
Switch(config-threshold)# aps trigger
Switch(config-threshold)# exit
Switch(config-t-list)# exit
Switch(config)# redundancy
Switch(config-red)# associate group sonet-channel
Switch(config-red-aps)# aps working transparent 3/0/0
Switch(config-red-aps)# aps protection transparent 3/0/0
```

```

Switch(config-red-aps)# aps y-cable
Switch(config-red-aps)# aps revertive
Switch(config-red-aps)# enable
Switch(config-red-aps)# exit
Switch(config-red)# exit
Switch(config)# interface transparent 3/0/0
Switch(config-if)# encaps sonet oc3
Switch(config-if)# monitor enable
Switch(config-if)# threshold-group sonet-alarms
Switch(config-if)# exit
Switch(config)# interface transparent 5/0/0
Switch(config-if)# encaps sonet oc3
Switch(config-if)# monitor enable
Switch(config-if)# threshold-group sonet-alarms

```

Displaying Alarm Threshold Configuration

To display the configuration of a threshold list and the threshold group for a transparent or wave interface, use the following EXEC commands:

Command	Purpose
show threshold-list [<i>name</i>]	Displays the threshold group configuration.
show interfaces { transparent <i>slot/subcard/0</i> wave <i>slot[/subcard]</i> }	Displays the transparent or wave interface configuration.

Examples

The following example shows how to display the configuration of a threshold group:

```

Switch# show threshold-list sonet-counters

Threshold List Name: sonet-counters
  Notification throttle timer : 5 (in secs)
  Threshold name : sonet-sdh section cv          Severity : Degrade
  Value : 10e-9
  APS Trigger : Not set
  Description : SONET BIP1 counter
  Threshold name : sonet-sdh section cv          Severity : Failure
  Value : 10e-6
  APS Trigger : Set
  Description : SONET BIP1 counter

```

The following example shows how to display the threshold group information for an interface:

```

Switch# show interfaces transparent 3/1/0
Transparent3/1/0 is up, line protocol is up
  Encapsulation: Sonet      Rate: oc3
  Signal monitoring: on
  Forward laser control: Off
  Configured threshold Group: sonet-counters
  Threshold monitored for: sonet-sdh section cv
  SF set value: 10e-8 (155 in 100 secs)
  SD set value: 10e-9 (155 in 1000 secs)
  Section code violation error count(bip1): 3713975925
  Number of errored seconds(es) : 57203
  Number of severely errored seconds(ses): 57203
  Number of severely errored framing seconds(sefs): 0
  Number of times SEF alarm raised: 0
  Number of times SF threshold exceeded: 0

```

```

Number of times SD threshold exceeded: 378
Loopback not set
Last clearing of "show interface" counters never
Hardware is transparent

```

About Laser Shutdown

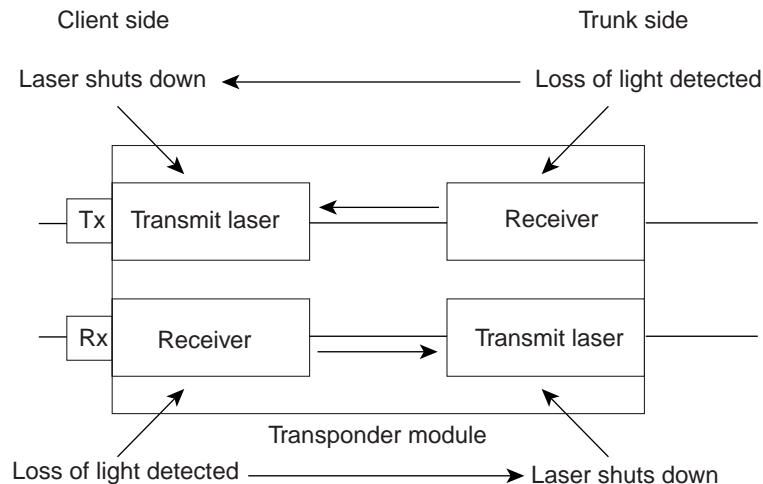
To avoid operator injury or transmission of unreliable data, or to provide quick path switchover, the Cisco ONS 15540 ESPx supports mechanisms to automatically shut down transponder module lasers. The three types of laser shutdown mechanisms are:

- Forward laser control (FLC)
- Open Fibre Control (OFC) safety protocol
- Laser safety control

About Forward Laser Control

When loss of light occurs on a receive interface (client, trunk, or intermediate) in a DWDM network, the corresponding transmitting laser on the far end of the network continues to function and may send unreliable information to the client. FLC provides a means to quickly shut down a transmitting laser when a receive signal failure occurs and pass the fault to the client devices (Figure 4-1). Loss of light can result from a failure in upstream optics or in the client equipment, a laser shutdown on an upstream node in the network, or a receiver failure in the module.

Figure 4-1 Forward Laser Control Overview



FLC works by optical shutdown or in-band signaling.

- In optical shutdown, all intermediate transmitters (lasers) are shut down when loss of light is detected. As a hop shuts down, the loss of light is passed to the next hop causing that hop to shut down. When a hop receives light causing its laser to restart, the signal is passed to the next hop, causing its laser to restart. Optical shutdown is used primarily by transparent transponders.

Optical shutdown is independent of service protocol. A disadvantage to optical shutdown is the delay caused by the shutdown and restart on the intermediate lasers. Services and clients that include shut/unshut of their transmitters in their link initialization protocol and that expect peer responses within the loop propagation delay may not be able to initialize their links through the DWDM with FLC enabled.

- In-band signaling occurs when a link break is detected by the edge DWDM device on the far end, but shutdown of the intermediate optics on the trunk is not done. This method is also referred to as end-to-end FLC or E2EFLC. The advantage of in-band signaling is that it provides faster loop response for fault propagation and restoration than regular FLC. Unlike optical shutdown, in-band signaling is protocol dependent and cannot be applied to generic or unknown traffic types. This method of FLC is used by specific protocol types on the transparent transponders and by aggregation cards on the Cisco ONS 15530.

FLC cannot be configured with OFC or ISC (Compatibility Mode). For the following services, the IOS software enables FLC in both directions during encapsulation configuration. In these cases, a user should not modify FLC:

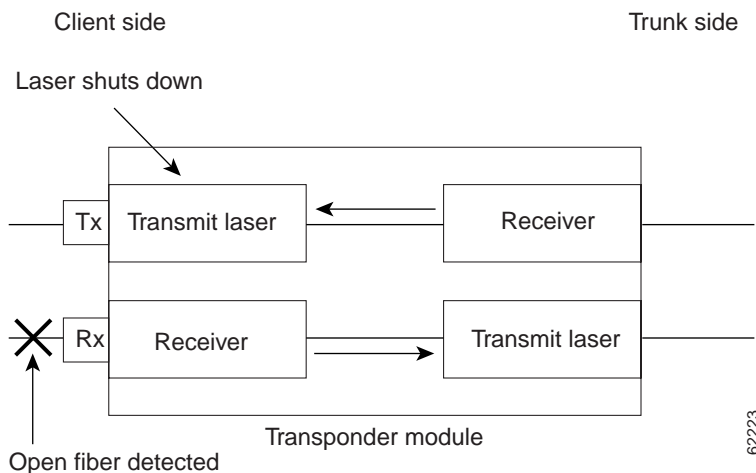
- Sysplex ETR
- Sysplex CLO
- Sysplex ISC peer mode
- All Y-cable automatic protection switching configurations

FLC is recommended for Gigabit Ethernet and FICON. For Gigabit Ethernet and FICON without FLC enabled, network fault propagation and recovery are dependent on the client device. Client fault propagation and detection may not work properly without FLC.

About Open Fibre Control

The Cisco ONS 15540 ESPx allows you to enable the OFC safety protocol on the client side interfaces. When the system detects an “open fiber,” the laser that transmits to the client equipment shuts down. An open fiber condition occurs when the connectors to the client equipment are detached from the transponder ports or when the fiber is cut (see Figure 4-2).

Figure 4-2 OFC Overview



The OFC safety protocol conforms to the Fibre Channel standard. It applies only to the Fibre Channel and ISC compatibility mode encapsulations. The Cisco ONS 15540 ESPx interoperates with OFC-standard-compliant client equipment.

**Caution**

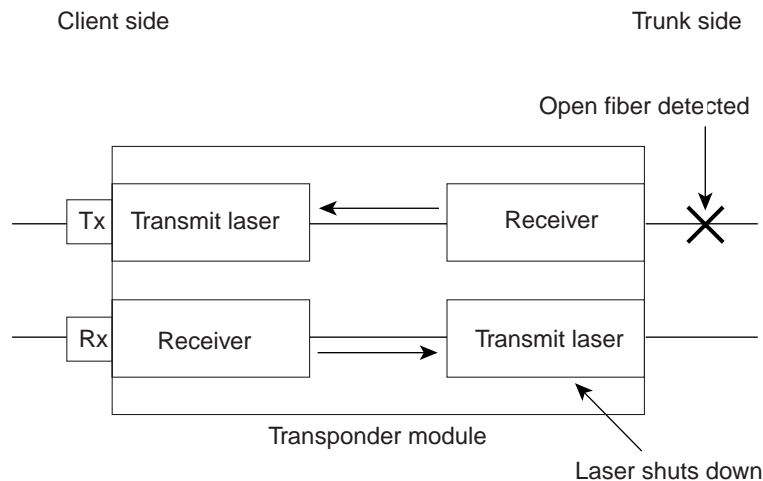
Do not configure OFC with either forward laser control or laser safety control. Combining these features interferes with the OFC protocol.

Use the **encapsulation** command, described in the “Configuring Protocol Encapsulation or Clock Rate” section on page 4-2 to configure OFC on a transparent interface.

About Laser Safety Control

The Cisco ONS 15540 ESPx allows you to enable laser safety control on the trunk side interfaces of the transponder modules. Much like OFC, the laser safety control protocol shuts down the transponder module laser transmitting to the trunk when a fiber cut occurs or when the trunk fiber is detached from the shelf (see Figure 4-3).

Figure 4-3 Laser Safety Control Overview



Laser safety control uses the same protocol state machine as OFC, but not the same timing. Laser safety control uses the pulse interval and pulse duration timers compliant with the ALS (automatic laser shutdown) standard (ITU-T G.664).

Use laser safety control with line card protected and unprotected configurations only. Enable laser safety control on all wave interfaces, including the OSC.

**Caution**

Laser safety control can interrupt signal transmission with splitter protected configurations. If you configure the system with splitter protection and enable laser safety control, the transmit laser to the client shuts down when an open fiber occurs on one transport fiber and signal transmission to the client is interrupted.

Configuring Laser Shutdown

This sections describes how to configure forward laser control and laser safety control on the Cisco ONS 15540 ESPx transponder module interfaces.



Note

To function correctly, configure forward laser control on both the transparent and wave interfaces on a transponder module. CSCdu42900

Configuring Forward Laser Control

To configure forward laser control on a transponder module transparent and wave interfaces, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface transparent <i>slot/subcard/port</i> Switch(config-if)#	Selects the transparent interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# [no] laser control forward enable	Configures forward laser control on the interface. The default state is disabled. Configuring FLC on the transparent interface shuts down the transparent interface laser when loss of light occurs on the trunk (wave) side.
Step 3	Switch(config-if)# exit	Returns to global configuration mode.
Step 4	Switch(config)# interface wave <i>slot/subcard</i> Switch(config-if)#	Selects the wave interface to configure and enters interface configuration mode.
Step 5	Switch(config-if)# [no] laser control forward enable	Configures forward laser control on the interface. The default state is disabled. Configuring FLC on the wave interface shuts down the wave interface laser when loss of light occurs on the client (transparent) side.



Caution

Do not configure forward laser control when OFC is enabled. Combining these features interferes with the OFC protocol.

Examples

The following example shows how to configure forward laser control for the transparent and wave interfaces on a transponder module:

```
Switch(config)# interface transparent 5/1/0
Switch(config-if)# laser control forward enable
Switch(config-if)# exit
Switch(config)# interface wave 5/1
Switch(config-if)# laser control forward enable
```

Displaying Forward Laser Control Configuration

To display the forward laser control configuration of a transparent or wave interface, use the following EXEC command:

Command	Purpose
show interfaces { transparent <i>slot/subcard/port</i> wave <i>slot/subcard</i> }	Displays interface information.

Example

The following example shows how to display the forward laser control configuration for an interface:

```
Switch# show interfaces transparent 10/0/0
Transparent10/0/0 is up, line protocol is up
  Encapsulation: Sonet      Rate: oc3
  Signal monitoring: off
  Time of last "monitor" state change never
  Time of last "encapsulation" change 10:18:20
  Forward laser control: On
  Configured threshold Group: None
  Loopback not set
  Last clearing of "show interface" counters 10:18:20
  Hardware is transparent
```

Configuring Laser Safety Control

To configure laser safety control on a wave interface, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface wave { <i>slot</i> <i>slot/subcard</i> }	Selects the wave interface to configure and enters interface configuration mode.
	Switch(config-if)#	
Step 2	Switch(config-if)# [no] laser control safety enable	Enables or disables laser safety control.



Note

Use laser safety control only with line card protected and unprotected configurations. Enable laser safety control on all the wave interfaces in the shelf, including the OSC.



Caution

Do not configure laser safety control when OFC is enabled. Combining these features interferes with the OFC safety protocol.

Example

The following example shows how to configure laser safety control on a wave interface:

```
Switch(config)# interface wave 8/0
Switch(config-if)# laser control safety enable
```

Displaying Laser Safety Control Configuration

To display the laser safety control configuration of a wave interface, use the following EXEC command:

Command	Purpose
show interfaces wave { <i>slot</i> <i>slot/subcard</i> }	Displays interface information.

Example

The following example shows how to display the laser safety control configuration for an interface:

```
Switch# show interfaces wave 3/1
launch2#show interfaces wave 10/0
Wave10/0 is up, line protocol is up
  Channel: 25   Frequency: 195.1 Thz   Wavelength: 1536.61 nm
  Splitter Protected: Yes
  Receiver power level: -10.0 dBm
  Laser safety control: On
  Forward laser control: Off
  Osc physical port: No
  Wavelength used for inband management: No
  Configured threshold Group: None
  Loopback not set
  Last clearing of "show interface" counters never
  Hardware is data_only_port
```

Configuring Transponder Channel Frequency

The transponders supported by the Cisco ONS 15540 ESPx transmits at one of two channel frequencies. You can select the channel frequency using the CLI (command-line interface). To change the channel frequency transmitted by the transponder module laser, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface wave <i>slot/subcard</i> Switch(config-if)#	Selects the wave interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# laser frequency <i>number</i>	Selects the frequency for the laser to transmit to the trunk. The default is the lower channel frequency for the transponder module.



Note

The laser requires approximately 10 seconds to change to the new frequency and stabilize. Any **laser frequency** commands entered during this time are ignored.

Example

The following example shows how to change the transponder channel frequency:

```
Switch(config)# interface wave 10/0
Switch(config-if)# laser frequency 192300
```


Displaying Transponder Channel Frequency

To display the channel frequency configuration, use the following EXEC command:

Command	Purpose
<code>show interfaces wave slot/subcard</code>	Displays the wave interface configuration.

Example

The following example shows how to verify the transponder channel frequency:

```
Switch# show interface wave 10/0
Wave10/0 is down, line protocol is down
  Channel: 30   Frequency: 195.7 THz   Wavelength: 1531.90 nm
  Active Wavepatch : Wavepatch10/0/0
  Splitter Protected: No
  Signal quality: Loss of light
  Receiver power level:
  Forward laser control: Off
  Laser safety control: Off
  Osc physical port: No
  Wavelength used for inband management: No
  Configured threshold Group: None
  Loopback not set
  Last clearing of "show interface" counters never
  Hardware is data_only_port
```

Configuring Optical Power Thresholds

Optical power thresholds provide a means of monitoring the signal power from the ITU laser. Four types of thresholds are provided:

- Low alarm
- Low warning
- High warning
- High alarm

When a threshold is crossed, the system sends a message to the console.



Note

The default values for the optical power receive thresholds are sufficient for most network configurations.

To configure optical power thresholds for a wavepatch interface on a transponder module, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface wavepatch <i>slot/subcard/port</i> Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# optical threshold power receive {low high} {alarm warning} value [severity {critical major minor not alarmed not reported}]	Specifies the optical power threshold value in units of 0.1 dBm. The default values are as follows: Low alarm: -28 dBm Low warning: -24 dBm High warning: -10 dBm High alarm: -8 dBm Alarm severity: major Warning severity: not alarmed

Examples

The following example shows how to configure optical power thresholds for a wavepatch interface on a transponder module:

```
Switch(config)# interface wavepatch 5/0/0
Switch(config-if)# optical threshold power receive high alarm -70
```

Displaying Optical Power Threshold Configuration

To display the optical power thresholds for a wavepatch interface, use the following EXEC command:

Command	Purpose
show interfaces wavepatch <i>slot/subcard/port</i>	Displays interface information.

Example

The following example shows how to display the forward laser control configuration for an interface:

```
Switch# show interfaces wavepatch 4/0/0
Wavepatch4/0/0 is up, line protocol is up
Receiver power level: -23.91 dBm
Optical threshold monitored for : Receive Power (in dBm)
Low alarm value = -28.0 (default)
Low Alarm Severity = major
Low warning value = -24.0 (default)
Low Warning Severity = not alarmed
High alarm value = -8.0 (default)
High Alarm Severity = major
High warning value = -10.0 (default)
High Warning Severity = not alarmed
Hardware is passive_port
```

About Patch Connections

Because the mux/demux modules are passive devices, the Cisco ONS 15540 ESPx does not detect its optical patch connection configuration. For system management purposes, you must also configure the patch connection configuration using the CLI.



Note

If you correctly patched your mux/demux modules, mux/demux motherboards, and line card motherboards, no CLI configuration is necessary for the signal to pass from the client to the trunk fiber.

Table 4-4 describes the types of patch connections on the Cisco ONS 15540 ESPx.

Table 4-4 Patch Connection Types

Patch Connection	Description
Thru interface to wdm interface or wdm interface to thru interface	Connection between two add/drop mux/demux modules in the same chassis slot
Thru interface to thru interface	Connection between two add/drop mux/demux modules in different chassis slots
OSC wave interface to OSC oscfilter interface or OSC oscfilter interface to OSC wave interface	Connection between the OSC wave interface on a mux/demux motherboard and the OSC oscfilter interface on the mux/demux module in the same chassis slot
Wavepatch interface to filter interface or filter interface to wavepatch interface	Connection between a wavepatch interface on a line card motherboard and a filter interface on a mux/demux module or a mux/demux motherboard

For more information on patch connection rules, refer to the *Cisco ONS 15540 ESPx Planning Guide*.

Configuring Patch Connections

To configure patch connections between mux/demux modules within the same shelf, use the following global configuration commands:

Command	Purpose
patch thru <i>slot/subcard1</i> wdm <i>slot/subcard2</i> or patch wdm <i>slot/subcard1</i> thru <i>slot/subcard2</i>	Configures the patch connection between two add/drop mux/demux modules in the same chassis slot.
patch thru <i>slot1/subcard1</i> thru <i>slot2/subcard2</i>	Configures the patch connection between two add/drop mux/demux modules in different chassis slots.
patch filterband <i>slot1/subcard1/port1</i> filtergroup <i>slot2/subcard2/port2</i> or patch filtergroup <i>slot1/subcard1/port1</i> filterband <i>slot2/subcard2/port2</i>	Configures the patch connection between a terminal mux/demux module supporting channels 1 through 16 and a terminal mux/demux module supporting channels 17 through 32 in the same chassis slot or in different chassis slots.

Command	Purpose
<p>patch wave <i>slot oscfilter slot/subcard</i></p> <p>or</p> <p>patch oscfilter <i>slot/subcard wave slot</i></p>	<p>Configures the patch connection between an OSC wave interface on a mux/demux motherboard and an OSC oscfilter interface on a mux/demux module in the same chassis slot.</p> <p>Note Correct patch command configuration for the oscfilter and OSC wave interfaces is required for bidirectional APS to function over the OSCP (see the “About Path Switching” section on page 7-17).</p>
<p>patch wavepatch <i>slot1/subcard1/port1 filter slot2/subcard2/port2</i></p> <p>or</p> <p>patch filter <i>slot1/subcard1/port1 wavepatch slot2/subcard2/port2</i></p>	<p>Configures the patch connection between a wavepatch interface on the line card motherboard and a filter interface on a mux/demux module or a mux/demux motherboard (Cisco ONS 15540 ESPx only).</p>

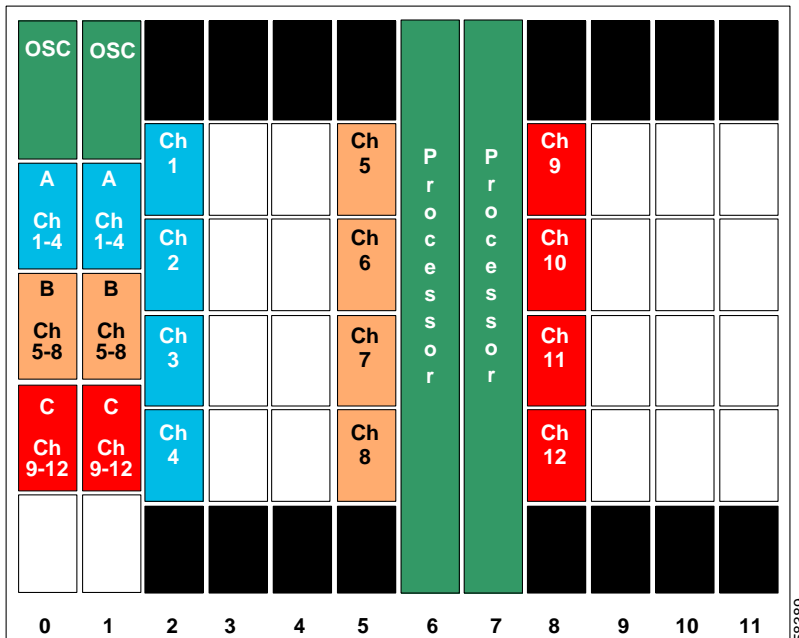


Note

If you correctly patch your mux/demux modules, **patch** command configuration is not necessary for the signal to pass from the client to the trunk fiber. However, without correct **patch** command configuration, CDP is unable to locate the wdm interfaces that connect to the trunk fiber and discover the topology neighbors. For more information on network monitoring, see the “Configuring CDP” section on page 11-3.

Figure 4-4 shows an example of a shelf configured with splitter protection for 12 channels.

Figure 4-4 Example Splitter Protected Shelf Configuration



The line card motherboards directly connect to the optical filter connectors on the mux/demux modules.

Example

The following example shows how to configure the patch connections between OSC interfaces, between mux/demux modules, and between the line card motherboards and the mux/demux modules in Figure 4-4:

```
Switch# configure terminal
Switch(config)# patch thru 0/0 wdm 0/1
Switch(config)# patch thru 0/1 wdm 0/2
Switch(config)# patch thru 0/2 thru 1/0
Switch(config)# patch thru 1/1 wdm 1/0
Switch(config)# patch thru 1/2 wdm 1/1
Switch(config)# patch wave 0 oscfilter 0/0
Switch(config)# patch wave 1 oscfilter 1/2
Switch(config)# patch wavepatch 2/0/0 filter 0/0/0
Switch(config)# patch wavepatch 2/1/0 filter 0/0/1
Switch(config)# patch wavepatch 2/2/0 filter 0/0/2
Switch(config)# patch wavepatch 2/3/0 filter 0/0/3
Switch(config)# patch wavepatch 2/0/1 filter 1/0/0
Switch(config)# patch wavepatch 2/1/1 filter 1/0/1
Switch(config)# patch wavepatch 2/2/1 filter 1/0/2
Switch(config)# patch wavepatch 2/3/1 filter 1/0/3
Switch(config)# patch wavepatch 5/0/0 filter 0/1/0
Switch(config)# patch wavepatch 5/1/0 filter 0/1/1
Switch(config)# patch wavepatch 5/2/0 filter 0/1/2
Switch(config)# patch wavepatch 5/3/0 filter 0/1/3
Switch(config)# patch wavepatch 5/0/1 filter 1/1/0
Switch(config)# patch wavepatch 5/1/1 filter 1/1/1
Switch(config)# patch wavepatch 5/2/1 filter 1/1/2
Switch(config)# patch wavepatch 5/3/1 filter 1/1/3
Switch(config)# patch wavepatch 8/0/0 filter 0/2/0
Switch(config)# patch wavepatch 8/1/0 filter 0/2/1
Switch(config)# patch wavepatch 8/2/0 filter 0/2/2
Switch(config)# patch wavepatch 8/3/0 filter 0/2/3
Switch(config)# patch wavepatch 8/0/1 filter 1/2/0
Switch(config)# patch wavepatch 8/1/1 filter 1/2/1
Switch(config)# patch wavepatch 8/2/1 filter 1/2/2
Switch(config)# patch wavepatch 8/3/1 filter 1/2/3
```

Displaying Patch Connections

To display the patch connections, use the following privileged EXEC command:

Command	Purpose
<code>show patch [detail]</code>	Displays the patch connections.

**Note**

The error field in the `show patch` command output helps troubleshoot shelf misconfigurations. When there is a channel mismatch between a transponder module and a mux/demux module, “Channel Mismatch” appears for the patch connection. When more than one mux/demux module drops the same channels, “Channel Mismatch” appears for all patch connections.

Example

The following example shows the patch connections:

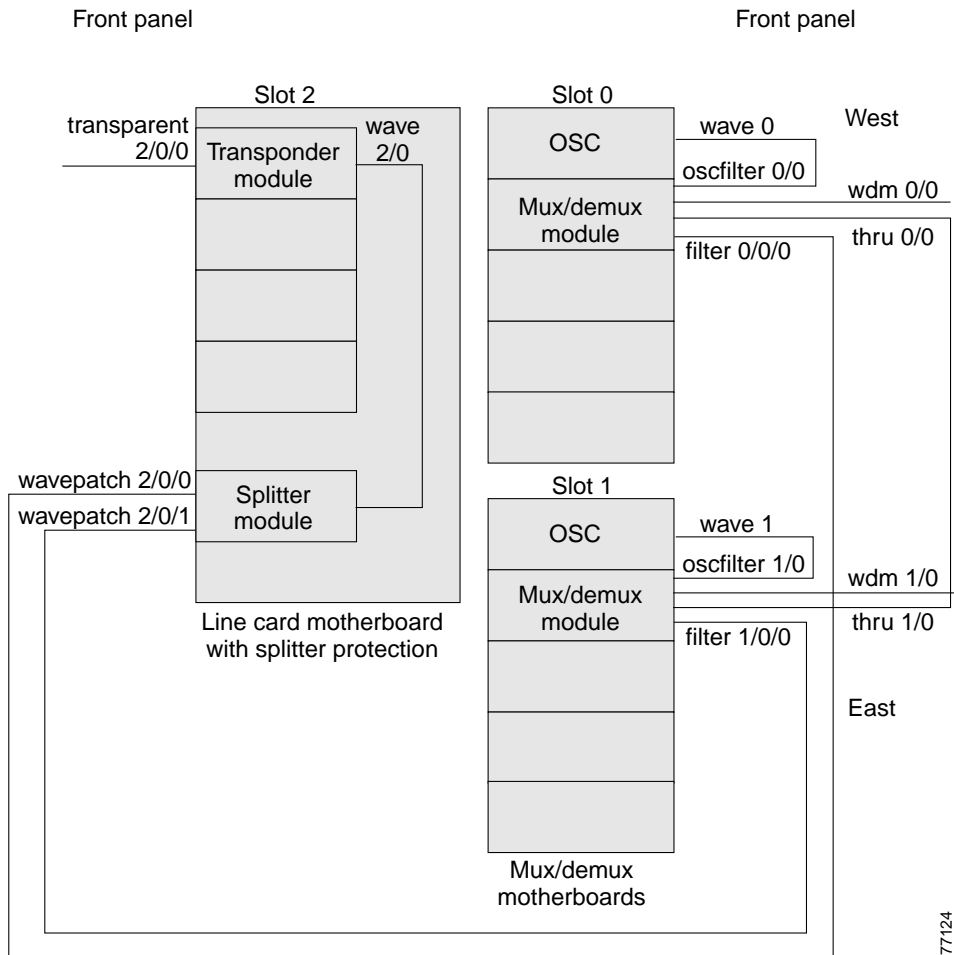
```
Switch# show patch
```

Patch Interface	Patch Interface	Type	Error
-----	-----	----	----
Thru0/0	Wdm0/1	USER	
Thru0/1	Wdm0/2	USER	
Thru0/2	Thru1/0	USER	
Thru1/1	Wdm1/0	USER	
Thru1/2	Wdm1/1	USER	
Wave0	Oscfilter0/0	USER	
Wave1	Oscfilter1/2	USER	

About Cross Connections

The client signal follows a path of optical cross connections through the Cisco ONS 15540 ESPx. Figure 4-5 shows an example of cross connections. Knowing the path of a signal through the shelf helps with system management and troubleshooting.

Figure 4-5 Optical Cross Connection Example on the Cisco ONS 15540 ESPx



Displaying Cross Connections

To display the signal path cross connections, use the following privileged EXEC command:

Command	Purpose
show connect [<i>edge</i> <i>intermediate</i> [<i>sort-channel</i> <i>interface</i> { <i>transparent slot/subcard/port</i> <i>wave slot/subcard</i> }]]	Displays the optical connections.

Examples

The following example shows the cross connections within a system configured for splitter protection:

```
Switch# show connect intermediate
client/      wave      wave      wdm
wave        client    patch    filter  trk  channel
-----
Trans2/0/0   Wave2/0   2/0/0*   0/0/0   0/0   1
              2/0/1   1/0/0   1/0     1/0   1
Trans2/2/0   Wave2/2   2/2/0*   0/0/2   0/0   3
              2/2/1   1/0/2   1/0     1/0   3
Trans2/3/0   Wave2/3   2/3/0*   0/0/3   0/0   4
              2/3/1   1/0/3   1/0     1/0   4
```

The following example shows the cross connections within a system configured for line card protection using splitter protected line card motherboards:

```
Switch# show connect intermediate
client/      wave      wave      wdm
wave        client    patch    filter  trk  channel
-----
Trans10/0/0  Wave10/0  10/0/0*  0/3/0   0/2   25
              10/0/1
Trans10/1/0  Wave10/1  10/1/0*  0/3/1   0/2   26
              10/1/1
Trans10/2/0  Wave10/2  10/2/0*  0/3/2   0/2   27
              10/2/1
Trans10/3/0  Wave10/3  10/3/0*  0/3/3   0/2   28
              10/3/1
```

About Performance History Counters

Cisco ONS 15540 ESPx supports 15 minute based performance history counters. You can use the performance history counters to track the performance of the Cisco ONS 15540 ESPx interfaces.

There are three types of performance history counters: current, 15-minute history, and 24-hour. Cisco ONS 15540 ESPx uses these counters to store the performance data for the following time periods:

- The current 15 minutes (using the current counter).
- The last 24 hours (using ninety six 15-minute history counters).
- The previous 1 day (using the 24-hour counter).

When the Cisco ONS 15540 ESPx system boots up, a continuously incrementing current counter is started. At the end of 15 minutes, this current counter is converted to a static 15-minute history counter with an interval number 1, and a new current counter is started with an interval number 2.

This process continues for 24 hours, by the end of which, ninety six 15-minute history counters are created. After the creation of the ninety sixth 15-minute history counter, a new 24-hour counter is created along with a current counter that has an interval number 1. The 24-hour counter has the aggregated data of all the ninety six 15-minute history counters.

The 15-minute history counters that are created thereafter overwrite the existing set of ninety six 15-minute history counters, in the order they were created. Again, after the creation of the ninety sixth 15-minute history counter, the contents of the existing 24-hour counter are overwritten with new values. This entire process continues in a cyclic fashion.

**Note**

The performance history counters are reset if you reboot the Cisco ONS 15540 ESPx system, insert or remove the line card or SFP online, or change the encapsulation.

The performance history counters synchronize periodically from the primary CPU switch module to the standby CPU switch module enabling the system to preserve the performance data across a CPU switch module switchover.

**Note**

To enable or disable the syncing of the performance history counters to the standby CPU switch module, execute the **auto-sync counter interfaces** command.

Displaying Performance History Counters

To display the performance history counters, use the following EXEC commands:

Command	Purpose
show performance current [<i>interface</i>]	Displays the current counter for the specified interface ¹ .
show performance history [<i>interface</i>] [<i>interval number</i>]	Displays the 15-minute history counter for the specified interface and interval number ¹ .
show performance 24-hour [<i>interface</i>]	Displays the 24-hour counter for the specified interface ¹ .

1. If you do not specify the interface or interval number, the performance history counters for all interfaces or interval numbers are displayed.

To clear and reset all performance history counters, use the following EXEC command:

Command	Purpose
clear performance history [<i>interface</i>]	Clears the performance history counters for the specified interface.

Performance history counters are supported only for the ESCON, FC, FICON, Gigabit Ethernet, and Sysplex ISC encapsulations on the transparent interface. The wave interface counters are not supported.

Examples

The following example shows how to display the current counter for a transparent interface:

```
Switch# show performance current transparent 2/0/0
Current 15 minute performance register
-----
Interface      : Transparent2/0/0
Interval Number : 32

Elapsed Time(seconds) : 715
Valid Time(seconds)   : 715

Code violation and running disparity error count : 0
```

The following example shows how to display the 15-minute history counter for a transparent interface:

```
Switch# show performance history transparent 2/0/0 10
15 minute performance history register
-----
Interface      : Transparent2/2/0
Interval Number : 10

Total Time(seconds) : 900
Valid Time(seconds) : 900

Code violation and running disparity error count : 0
```

The following example shows how to display the 24-hour counter for a transparent interface:

```
Switch# show performance 24-hour transparent 2/0/0
24 hour performance register
-----
Interface      : Transparent2/0/0

Total Time(seconds) : 86400
Valid Time(seconds) : 86400

Code violation and running disparity error count : 0
```




Configuring 10-GE Transponder Module Interfaces and Patch Connections

This chapter describes how to configure interfaces and patch connections on the Cisco ONS 15540 ESPx. This chapter includes the following sections:

- Enabling Tengigethernetphy Interfaces, page 5-2
- Enabling the In-Band Message Channel on Tengigethernetphy Interfaces, page 5-3
- Enabling Waveethernetphy Interfaces and Turning on ITU Lasers, page 5-4
- Configuring Loopbacks, page 5-5
- About Alarm Thresholds, page 5-7
- Configuring Alarm Thresholds, page 5-7
- Configuring Forward Laser Control, page 5-11
- Configuring Patch Connections, page 5-12
- Configuring Optical Power Thresholds, page 5-14
- Turning Lasers On and Off, page 5-15
- About Cross Connections, page 5-16
- About Performance History Counters, page 5-17
- Displaying Performance History Counters, page 5-18



Note

To ensure the installed Cisco IOS software supports your hardware and provides the software features you wish to use, see the “New and Changed Information” section on page xviii. Also refer to the “Hardware Supported” section and “Feature Set” section of the latest release notes for the Cisco ONS 15540 ESPx.

To configure tengigethernetphy interfaces on the Cisco ONS 15540 ESPx, perform the following steps:

- Step 1** Enable the interface (required).
- Step 2** Enable the in-band message channel (optional).
- Step 3** Configure loopback (optional).
- Step 4** Create alarm threshold lists and apply them to the interfaces (optional).

Step 5 Enable forward laser control (optional).

To configure waveethernetphy interfaces on the Cisco ONS 15540 ESPx, perform the following steps:

Step 1 Enable the interface and turn on the ITU laser (required).

Step 2 Enable forward laser control (optional).

Step 3 Configure loopback (optional).

Step 4 Create alarm threshold lists and apply them to the interfaces (optional).

To configure wavepatch interfaces on the Cisco ONS 15540 ESPx, perform the following steps:

Step 1 Configure the patch connections (required).

Step 2 Configure the optical power receive threshold (optional).

Enabling Tengigethernetphy Interfaces

To enable the 10-GE transponder module tengigethernetphy interfaces, perform the following tasks, starting in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface tengigethernetphy slot/subcard Switch(config-if)#	Specifies an interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# no shutdown	Enables the interface.
Step 3	Switch(config-if)# no laser shutdown	Turns on the client-side laser.

Example

The following example shows how to enable a tengigethernetphy interface:

```
Switch(config)# interface tengigethernetphy 10/0
Switch(config-if)# no shutdown
```

Displaying Tengigethernetphy Interface Information

The following example shows how to display tengigethernetphy interface information.

```
Switch# show interface tengigethernetphy 10/0
TenGigEthernetPhy10/0 is up, line protocol is up
  Signal quality      : Loss of lock
  Laser shut down    : No
  Forward laser control : Off
  CDL Enabled        : Yes
```

```

Configured threshold Group: thresh
Threshold monitored for: 64b66b cvrd
SF set value: 10e-4 (1249438 in 1 secs)
SD set value: 10e-5 (124994 in 1 secs)
Code violation and running disparity error count( 64b66b cvrd): 0
Number of times SF threshold exceeded: 0
Number of times SD threshold exceeded: 0
TenGige Non CDL Pkt count: 0
CDL HEC error count: 0
TenGige CDL idle Pkt count: 0

Defect Indication Status      : up
Configured Node Behavior      : Hop Terminating
Current Node Behavior         : Hop Terminating
Defect Indication Receive     : None
Defect Indication Transmit    : FDI-E BDI-H
Loopback set
Last clearing of "show interface" counters never
Hardware is data_enabled_port

```

Enabling the In-Band Message Channel on Tengigethernetphy Interfaces

The tengigethernetphy interface will support in-band message channel traffic when a system connected to the 10-GE transponder module also supports the in-band message channel. When the in-band message channel is enabled on a tengigethernetphy interface, an ethernetdcc interface becomes available for configuration. The identifier for this interface is ethernetdcc *slot/subcard/1*.

To enable the in-band message channel on tengigethernetphy interfaces, perform the following tasks, starting in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface tengigethernetphy <i>slot/subcard</i>	Specifies an interface to configure and enters interface configuration mode.
	Switch(config-if)#	
Step 2	Switch(config-if)# cdl enable	Enables the in-band message channel on a tengigethernetphy interface. The default is disabled.

To configure the ethernetdcc *slot/subcard/1* interface, refer to the “Configuring IP on Ethernetdcc Interfaces for the In-Band Message Channel” section on page 11-11.



Note

The in-band message channel must be enabled on both systems to function correctly.

Example

The following example shows how to enable the in-band message channel on a tengigethernetphy interface:

```

Switch(config)# interface tengigethernetphy 10/0
Switch(config-if)# no shutdown

```

Displaying the In-Band Message Channel Configuration

The following example shows how to display the in-band message channel configuration on a tengigethernetphy interface.

```
Switch# show interface tengigethernetphy 10/0
TenGigEthernetPhy10/0 is up, line protocol is up
  Signal quality      : Loss of lock
  Laser shut down    : No
  Forward laser control : Off
→ CDL Enabled       : Yes

  Configured threshold Group: thresh
  Threshold monitored for: 64b66b cvrd
  SF set value: 10e-4 (1249438 in 1 secs)
  SD set value: 10e-5 (124994 in 1 secs)
  Code violation and running disparity error count ( 64b66b cvrd): 0
  Number of times SF threshold exceeded: 0
  Number of times SD threshold exceeded: 0
  TenGige Non CDL Pkt count: 0
  CDL HEC error count: 0
  TenGige CDL idle Pkt count: 0

  Defect Indication Status      : up
  Configured Node Behavior      : Hop Terminating
  Current Node Behavior         : Hop Terminating
  Defect Indication Receive     : None
  Defect Indication Transmit    : FDI-E BDI-H
  Loopback set
  Last clearing of "show interface" counters never
  Hardware is data_enabled_port
```

Enabling Waveethernetphy Interfaces and Turning on ITU Lasers

The waveethernetphy interface is the trunk side interface for the 10-GE transponder module that corresponds to the ITU laser. It supports the in-band message channel and is associated with the ethernetdcc *slot/subcard/0* interface.

To enable the 10-GE transponder module waveethernetphy interface and turn on the ITU laser, perform the following tasks, starting in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface waveethernetphy <i>slot/subcard</i> Switch(config-if)#	Specifies an interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# no shutdown	Enables the interface.
Step 3	Switch(config-if)# no laser shutdown	Turns on the ITU laser.

To configure the ethernetdcc *slot/subcard/0* interface, refer to the “Configuring IP on Ethernetdcc Interfaces for the In-Band Message Channel” section on page 11-11.

Example

The following example shows how to enable a waveethernetphy interface:

```
Switch(config)# interface waveethernetphy 10/0
Switch(config-if)# no shutdown
```

Displaying Waveethernetphy Interface Information

The following example shows how to display waveethernetphy interface information.

```
Switch# show interface waveethernetphy 10/0
WaveEthernetPhy10/0 is up, line protocol is up
  Channel: 26   Frequency: 195.2 Thz   Wavelength: 1535.82 nm
  Active Wavepatch      : Wavepatch4/1/0
  Splitter Protected    : No
  Signal quality        : Loss of lock
  Receive power level   : -30.0 dBm
  Transmit condition    : Good
  Laser shut down       : No
  Forward laser control : Off
  Osc physical port     : No
  Wavelength used for inband management: No
  Loopback not set

  Configured threshold Group: thresh
  Threshold monitored for: 64b66b cvrd
  SF set value: 10e-4 (1249438 in 1 secs)
  SD set value: 10e-5 (124994 in 1 secs)
  Code violation and running disparity error count( 64b66b cvrd): 0
  Number of times SF threshold exceeded: 0
  Number of times SD threshold exceeded: 0
  TenGige Non CDL Pkt count: 0
  CDL HEC error count: 0
  TenGige CDL idle Pkt count: 0

  Defect Indication Status      : up
  Configured Node Behavior      : Hop Terminating
  Current Node Behavior         : Hop Terminating
  Defect Indication Receive     : None
  Defect Indication Transmit    : FDI-E BDI-H

  Last clearing of "show interface" counters never
  Hardware is data_and_cdl_enabled_port
```

Configuring Loopbacks

The Cisco ONS 15540 ESPx software allows you to configure interface loopback using the CLI. You can use this feature to test and troubleshoot interfaces without physically looping them back.

To configure a loopback on 10-GE transponder module interfaces, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface { waveethernetphy slot/subcard tengigethernetphy slot/subcard }	Specifies an interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# loopback	Configures a software loopback on the interface.



Note Loop back either the waveethernetphy interface or the tengigethernetphy interface on a given module, but not both at the same time.

Displaying Loopback Configuration

To display the loopback configuration for a tengigethernetphy or waveethernetphy interface, use the following EXEC command:

Command	Purpose
show interfaces { tengigethernetphy slot/subcard waveethernetphy slot/subcard }	Displays the tengigethernetphy or waveethernetphy interface configuration.

Example

The following example shows how to display the loopback configuration for a tengigethernetphy interface:

```
Switch# show interfaces tengigethernetphy 10/0
TenGigEthernetPhy10/0 is up, line protocol is up
  Signal quality      : Loss of lock
  Laser shut down    : No
  Forward laser control : Off
  CDL Enabled        : Yes

Configured threshold Group: tengig-counters
Threshold monitored for: 64b66b cvrd
SF set value: 10e-4 (1249438 in 1 secs)
SD set value: 10e-5 (124994 in 1 secs)
Code violation and running disparity error count ( 64b66b cvrd): 0
Number of times SF threshold exceeded: 0
Number of times SD threshold exceeded: 0
TenGige Non CDL Pkt count: 0
CDL HEC error count: 0
TenGige CDL idle Pkt count: 0

Defect Indication Status      : up
Configured Node Behavior      : Hop Terminating
Current Node Behavior          : Hop Terminating
Defect Indication Receive     : None
Defect Indication Transmit    : FDI-E BDI-H
→ Loopback set
Last clearing of "show interface" counters never
Hardware is data_enabled_port
```


The following example shows how to display the loopback configuration on a waveethernetphy interface.

```
Switch# show interface waveethernetphy 10/0
WaveEthernetPhy10/0 is up, line protocol is up
  Channel: 26   Frequency: 195.2 Thz   Wavelength: 1535.82 nm
  Active Wavepatch      : Wavepatch4/1/0
  Splitter Protected    : No
  Signal quality        : Loss of lock
  Receive power level   : -30.0 dBm
  Transmit condition    : Good
  Laser shut down       : No
  Forward laser control : Off
  Osc physical port     : No
  Wavelength used for inband management: No
  Defect Indication Transmit : FDI-E BDI-H
→ Loopback not set

Configured threshold Group: thresh
Threshold monitored for: 64b66b cvrd
SF set value: 10e-4 (1249438 in 1 secs)
SD set value: 10e-5 (124994 in 1 secs)
Code violation and running disparity error count( 64b66b cvrd): 0
Number of times SF threshold exceeded: 0
Number of times SD threshold exceeded: 0
TenGige Non CDL Pkt count: 0
CDL HEC error count: 0
TenGige CDL idle Pkt count: 0

< Information deleted >
```

About Alarm Thresholds

You can configure thresholds on tengigethernetphy and waveethernetphy interfaces that issue alarm messages to the system if the thresholds are exceeded. Every second, the monitoring facility updates the counters that correspond to the alarm thresholds. When the signal degrades, or fails entirely, the system issues alarms to the console. These alarms can help isolate failures in the system and in the network.

You can configure more than one threshold list on an interface. The threshold lists cannot have overlapping counters so that only one counter is set for the interface. Also, the threshold list name cannot begin with the text string “default” because the it is reserved for use by the system.

Configuring Alarm Thresholds

To configure alarm thresholds on tengigethernetphy and waveethernetphy interfaces, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# threshold-list <i>name</i> Switch(config-t-list)#	Creates or selects the threshold list to configure and enters threshold list configuration mode. Note You cannot modify an existing threshold list if it is associated with an interface.
Step 2	Switch(config-t-list)# notification-throttle timer <i>seconds</i>	Configures the SNMP notification timer. The default value is 5 seconds. (Optional)

	Command	Purpose
Step 3	Switch(config-t-list)# threshold name { cvr cdl hec crc sonet-sdh section cv tx-crc } { failure degrade } [index value] Switch(config-threshold)#	Specifies a threshold type to modify and enters threshold configuration mode.
Step 4	Switch(config-threshold)# value rate value	Specifies the threshold rate value. This value is the negative power of 10 (10 ⁻ⁿ).
Step 5	Switch(config-threshold)# description text	Specifies a description of the threshold. The default value is the null string. (Optional)
Step 6	Switch(config-threshold)# aps trigger	Enables APS switchover when this threshold is crossed. (Optional) Note This command only triggers switchovers for y-cable protection, not for splitter protection.
Step 7	Switch(config-threshold)# exit Switch(config-t-list)#	Returns to threshold list configuration mode. Repeat Step 3 through Step 7 to configure more thresholds in the threshold list.
Step 8	Switch(config-t-list)# exit Switch(config)#	Returns to global configuration mode.
Step 9	Switch(config)# interface { tengigethernetphy slot/subcard waveethernetphy slot/subcard } Switch(config-if)#	Selects the tengigethernetphy or waveethernetphy interface to configure and enters interface configuration mode.
Step 10	Switch(config-if)# threshold-group name	Configures the threshold list on the interface.



Note If a threshold type does not apply to the 10-GE protocol, that threshold type is ignored.

Table 5-2 lists the threshold error rates in errors per second.

Table 5-1 Threshold Error Rates for Monitored Protocols in Errors Per Second

Rate	SONET OC-3 or SDH STM-1	SONET OC-12 or SDH STM-4	SONET OC-48 or SDH STM-16	Gigabit Ethernet	ESCON	FICON	Fibre Channel ¹
3	31753	32000	32000	1244390	199102	1057731	1057731
4	12318	27421	31987	124944	19991	106202	106202
5	1518	5654	17296	12499	2000	10625	10625
6	155	616	2394	1250	200	1062	1062
7	15.5	62	248	125	20	106	106
8	1.55	6.2	24.8	12.5	2	10.6	10.6
9	0.155	0.62	2.48	1.25	0.2	1.06	1.06

1. Only the 1 Gbps rate is monitored.

Table 5-2 **Thresholds for Monitored Protocols (Errors Per Second)**

Rate	10-Gigabit Ethernet CVRD	10-Gigabit Ethernet CDL HEC
3	12,443,900	6512
4	1,249,438	665
5	124,944	67
6	10,312	7
7	1031	0.7
8	103	0.07
9	10	0.007

Examples

The following example shows how to create an alarm threshold list and configure that list on a tengigethernetphy interface:

```
Switch# configure terminal
Switch(config)# threshold-list tengig-counters
Switch(config-t-list)# threshold name cvrd degrade
Switch(config-threshold)# value rate 5
Switch(config-threshold)# exit
Switch(config-t-list)# threshold name cvrd failure
Switch(config-threshold)# value rate 4
Switch(config-threshold)# exit
Switch(config-t-list)# exit
Switch(config)# interface tengigethernetphy 10/0
Switch(config-if)# threshold-group tengig-counters
```

The following example shows how to create an alarm threshold list with the APS switchover trigger and configure that list on a pair of associated tengigethernetphy interfaces:

```
Switch(config)# threshold-list tengig-alarms
Switch(config-t-list)# threshold name cvrd failure
Switch(config-threshold)# value rate 6
Switch(config-threshold)# aps trigger
Switch(config-threshold)# exit
Switch(config-t-list)# exit
Switch(config)# redundancy
Switch(config-red)# associate group tengig-channel
Switch(config-red-aps)# aps working tengigethernetphy 3/0
Switch(config-red-aps)# aps protection tengigethernetphy 5/0
Switch(config-red-aps)# aps y-cable
Switch(config-red-aps)# aps enable
Switch(config-red-aps)# exit
Switch(config-red)# exit
Switch(config)# interface tengigethernetphy 3/0
Switch(config-if)# no shutdown
Switch(config-if)# threshold-group tengig-alarms
Switch(config-if)# exit
Switch(config)# interface tengigethernetphy 5/0
Switch(config-if)# no shutdown
Switch(config-if)# threshold-group tengig-alarms
```

Displaying Alarm Threshold Configuration

To display the configuration of a threshold list and the threshold group for a tengigethernetphy or waveethernetphy interface, use the following EXEC commands:

Command	Purpose
show threshold-list [<i>name</i>]	Displays the threshold group configuration.
show interfaces { <i>tengigethernetphy slot/subcard</i> <i>waveethernetphy slot/subcard</i> }	Displays the tengigethernetphy or waveethernetphy interface configuration.

Example

The following example shows how to display the configuration of a threshold group:

```
Switch# show threshold-list tengig-counters

Threshold List Name: tengig-counters
  Notification throttle timer : 5 (in secs)
  Threshold name : cvrd          Severity : Degrade
    Value : 10e-5
    APS Trigger : Not set
  Threshold name : cvrd          Severity : Failure
    Value : 10e-4
    APS Trigger : Not set
```

The following example shows how to display the threshold group information for a tengigethernetphy interface:

```
Switch# show interfaces tengigethernetphy 10/0
TenGigEthernetPhy10/0 is up, line protocol is up
  Signal quality          : Loss of lock
  Laser shut down         : No
  Forward laser control   : Off
  CDL Enabled             : Yes

Configured threshold Group: tengig-counters
Threshold monitored for: 64b66b cvrd
SF set value: 10e-4 (1249438 in 1 secs)
SD set value: 10e-5 (124994 in 1 secs)
Code violation and running disparity error count( 64b66b cvrd): 0
Number of times SF threshold exceeded: 0
Number of times SD threshold exceeded: 0
TenGige Non CDL Pkt count: 0
CDL HEC error count: 0
TenGige CDL idle Pkt count: 0

Defect Indication Status      : up
Configured Node Behavior      : Hop Terminating
Current Node Behavior         : Hop Terminating
Defect Indication Receive     : None
Defect Indication Transmit    : FDI-E BDI-H
Loopback set
Last clearing of "show interface" counters never
Hardware is data_enabled_port
```

Configuring Forward Laser Control

To configure forward laser control on a 10-GE transponder module tengigethernetphy and waveethernetphy interfaces, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface tengigethernetphy slot/subcard Switch(config-if)#	Selects the tengigethernetphy interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# [no] laser control forward enable	Configures forward laser control on the interface. The default state is disabled. Configuring FLC on the tengigethernetphy interface shuts down the waveethernetphy interface laser when loss of light occurs on the client (tengigethernetphy) side. For more information, see the “About Forward Laser Control” section on page 4-13.
Step 3	Switch(config-if)# exit	Returns to global configuration mode.
Step 4	Switch(config)# interface waveethernetphy slot/subcard Switch(config-if)#	Selects the waveethernetphy interface to configure and enters interface configuration mode.
Step 5	Switch(config-if)# [no] laser control forward enable	Configures forward laser control on the interface. The default state is disabled. Configuring FLC on the waveethernetphy interface shuts down the tengigethernetphy interface laser when loss of light occurs on the trunk (waveethernetphy) side. For more information, see the “About Forward Laser Control” section on page 4-13.

Examples

The following example shows how to configure forward laser control for the tengigethernetphy and waveethernetphy interfaces on a 10-GE transponder module:

```
Switch(config)# interface tengigethernetphy 5/1
Switch(config-if)# laser control forward enable
Switch(config-if)# exit
Switch(config)# interface waveethernetphy 5/1
Switch(config-if)# laser control forward enable
```

Displaying Forward Laser Control Configuration

To display the forward laser control configuration of a tengigetheretnphy or waveetheretnphy interface, use the following EXEC command:

Command	Purpose
show interfaces { tengigetheretnphy <i>slot/subcard</i> waveetheretnphy <i>slot/subcard</i> }	Displays interface information.

Example

The following example shows how to display the forward laser control configuration for an interface:

```
Switch# show interfaces waveetheretnphy 10/0
TenGigEthernetPhy10/0 is up, line protocol is up
  Signal quality          : Loss of lock
  Laser shut down        : No
→ Forward laser control  : On
  CDL Enabled            : Yes

  Configured threshold Group: thresh
  Threshold monitored for: 64b66b cvrd
  SF set value: 10e-4 (1249438 in 1 secs)
  SD set value: 10e-5 (124994 in 1 secs)
  Code violation and running disparity error count( 64b66b cvrd): 0
  Number of times SF threshold exceeded: 0
  Number of times SD threshold exceeded: 0
  TenGige Non CDL Pkt count: 0
  CDL HEC error count: 0
  TenGige CDL idle Pkt count: 0

  Defect Indication Status      : up
  Configured Node Behavior      : Hop Terminating
  Current Node Behavior         : Hop Terminating
  Defect Indication Receive     : None
  Defect Indication Transmit    : FDI-E BDI-H
  Loopback set
  Last clearing of "show interface" counters never
  Hardware is data_enabled_port
```

Configuring Patch Connections

Because the mux/demux modules are passive devices, the Cisco ONS 15540 ESPx does not detect its optical patch connection configuration. For system management purposes, you must also configure the patch connections using the CLI.



Note

If you correctly patched your modules, no CLI configuration is necessary for the signal to pass from the client to the trunk fiber.

To configure patch connections, use the following global configuration commands:

Command	Purpose
patch wavepatch <i>slot/subcard/port filter slot/subcard/port</i> or patch filter <i>slot/subcard/port wavepatch slot/subcard/port</i>	Configures the patch connection between the wavepatch interface on a 10-Gbps line card motherboard and the filter interface on a mux/demux module.

**Note**

If you correctly patch your mux/demux modules, **patch** command configuration is not necessary for the signal to pass from the client to the trunk fiber. However, without correct **patch** command configuration, CDP is unable to locate the wdm interfaces that connect to the trunk fiber and discover the topology neighbors. For more information on network monitoring, see the “Configuring CDP” section on page 11-3.

Example

The following example shows how configure the patch connection between a 10-Gbps line card motherboard and a mux/demux module:

```
Switch# configure terminal
Switch(config)# patch wavepatch 10/0/0 filter 0/0/1
```

Displaying Patch Connections

To display the patch connections, use the following privileged EXEC command:

Command	Purpose
show patch [detail]	Displays the patch connections.

**Note**

The error field in the **show patch** command output helps troubleshoot shelf misconfigurations. When there is a channel mismatch between a 10-GE transponder module and a mux/demux module, “Channel Mismatch” appears for the patch connection. When more than one mux/demux module drops the same channels, “Channel Mismatch” appears for all patch connections.

Example

The following example shows the patch connections:

```
Switch# show patch
Patch Interface      Patch Interface      Type      Dir      Error
-----
Filter0/0/1         Wavepatch10/0/0     USER     Both
Oscfilter0/0        Wave0                USER     Both
Wdm0/0              Thru0/1             USER     Both
```

Configuring Optical Power Thresholds

Optical power thresholds provide a means of monitoring the signal power from the ITU laser. Four types of thresholds are provided:

- Low alarm
- Low warning
- High warning
- High alarm

When a threshold is crossed, the system sends a message to the console.



Note

The default values for the optical power receive thresholds are sufficient for most network configurations.

To configure optical power thresholds for wavepatch interfaces on a 10-GE transponder module, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface wavepatch <i>slot/subcard/port</i> Switch(config-if)#	Selects the transparent interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# optical threshold power receive {low high} {alarm warning} <i>value</i> [severity {critical major minor not alarmed not reported}]	Specifies the optical power threshold value in units of 0.1 dBm. The default values are as follows: Low alarm: -22 dBm Low warning: -20 dBm High warning: -10 dBm High alarm: -8 dBm Alarm severity: major Warning severity: not alarmed

Examples

The following example shows how to configure optical power thresholds for wavepatch interfaces on a 10-GE transponder module:

```
Switch(config)# interface wavepatch 5/0/0
Switch(config-if)# optical threshold power receive low alarm -210
```

Displaying Optical Power Threshold Configuration

To display the optical power thresholds for a wavepatch interface, use the following EXEC command:

Command	Purpose
show interfaces wavepatch <i>slot/subcard/port</i>	Displays interface information.

Example

The following example shows how to display the forward laser control configuration for an interface:

```
Switch# show interfaces wavepatch 10/0/0
Wavepatch10/0/0 is up, line protocol is up
  Receiver power level: -35.0 dBm

  Optical threshold monitored for : Receive Power (in dBm)
  Threshold exceeded for : Low Warning and Low Alarm
  Low alarm value           = -21.0
  Low Alarm Severity        = critical
  Low warning value         = -20.0 (default)
  Low Warning Severity      = not alarmed
  High alarm value          = -6.1
  High Alarm Severity       = critical
  High warning value        = -8.0 (default)
  High Warning Severity     = not alarmed
  Hardware is passive_port
```

Turning Lasers On and Off

When in-band message channel capable interfaces are administratively shut down using the **shutdown** command, data traffic is interrupted. To stop all traffic, you must turn off the laser.

To turn the lasers on and off on a 10-GE transponder module, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface { tengigethernetphy slot/subcard waveethernetphy slot/subcard } Switch(config-if)#	Selects the transparent interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# laser shutdown	Shuts down the laser.
Step 3	Switch(config-if)# no laser shutdown	Turns the laser on.

**Note**

The 10-GE laser must warm up for 2 minutes before carrying traffic when a **no laser shutdown** command is used on a tengigethernetphy interface.

Examples

The following example shows how to configure optical power thresholds for wavepatch interfaces on a 10-GE transponder module:

```
Switch(config)# interface waveethernetphy 10/0
Switch(config-if)# laser shutdown
```

Displaying Laser Status

To display the laser status, use the following EXEC command:

Command	Purpose
show interfaces { tengigetherne phy slot/subcard waveetherne phy slot/subcard}	Displays interface information.

Example

The following example shows how to display the forward laser control configuration for an interface:

```
Switch# show interfaces waveethernephy 10/0
WaveEthernetPhy10/0 is up, line protocol is up
  Channel: 26   Frequency: 195.2 Thz   Wavelength: 1535.82 nm
  Active Wavepatch      : Wavepatch4/1/0
  Splitter Protected    : No
  Signal quality        : Loss of lock
  Receive power level   : -35.0 dBm
  Transmit condition    : Good
→ Laser shut down      : No
  Forward laser control : Off
  Osc physical port     : No
  Wavelength used for inband management: No
  Loopback not set

  Configured threshold Group: thresh
  Threshold monitored for: 64b66b cvrd
  SF set value: 10e-4 (1249438 in 1 secs)
  SD set value: 10e-5 (124994 in 1 secs)
  Code violation and running disparity error count ( 64b66b cvrd): 0
  Number of times SF threshold exceeded: 0
  Number of times SD threshold exceeded: 0
  TenGige Non CDL Pkt count: 0
  CDL HEC error count: 0
  TenGige CDL idle Pkt count: 458745

  Defect Indication Status      : up
  Configured Node Behavior      : Hop Terminating
  Current Node Behavior         : Hop Terminating
  Defect Indication Receive     :          None
  Defect Indication Transmit    : FDI-E

  Last clearing of "show interface" counters never
  Hardware is data_and_cdl_enabled_port
```

About Cross Connections

The client signal follows a path of interface optical cross connections through the Cisco ONS 15540 ESPx. Knowing the path of a signal through the shelf helps with system management and troubleshooting.

Displaying Cross Connections

To display the signal path cross connections, use the following privileged EXEC command:

Command	Purpose
show connect [edge intermediate [sort-channel interface { tengigethernetphy <i>slot/subcard</i> waveethernetphy <i>slot/subcard</i> }]]	Displays the optical connections.

Examples

The following example shows the cross connections within a system configured for splitter protection:

```
Switch# show connect intermediate
client/      wave      wave      wdm
wave        client    patch    filter   trk   channel
-----
TenGE3/0    WaveE3/0  3/0/0*
Tran9/0/0   Wave9/0   9/0/0*
              9/0/1
Tran9/1/0   Wave9/1   9/1/0*
              9/1/1
Tran9/2/0   Wave9/2   9/2/0*
              9/2/1
Tran9/3/0   Wave9/3   9/3/0*
              9/3/1
Tran10/1/0  Wave10/1  10/1/0*
              10/1/1
Tran10/3/0  Wave10/3  10/3/0*
              10/3/1
TenGE11/0   WaveE11/0 11/0/0*  0/0/25  0/0   26
              11/0/1  1/3/1   1/3     26
```

The following example shows the cross connections within a system configured for line card protection using splitter protected 10-Gbps line card motherboards:

```
Switch# show connect intermediate
client/      wave      wave      wdm
wave        client    patch    filter   trk   channel
-----
TenGE10/0/0  WaveE10/0 10/0/0*  0/3/0   0/2   25
              10/0/1
TenGE10/1/0  WaveE10/1 10/1/0*  0/3/1   0/2   26
              10/1/1
TenGE10/2/0  WaveE10/2 10/2/0*  0/3/2   0/2   27
              10/2/1
TenGE10/3/0  WaveE10/3 10/3/0*  0/3/3   0/2   28
              10/3/1
```

About Performance History Counters

Cisco ONS 15540 ESPx supports 15 minute based performance history counters. You can use the performance history counters to track the performance of the Cisco ONS 15540 ESPx interfaces.

There are three types of performance history counters: current, 15-minute history, and 24-hour. Cisco ONS 15540 ESPx uses these counters to store the performance data for the following time periods:

- The current 15 minutes (using the current counter).

- The last 24 hours (using ninety six 15-minute history counters).
- The previous 1 day (using the 24-hour counter).

When the Cisco ONS 15540 ESPx system boots up, a continuously incrementing current counter is started. At the end of 15 minutes, this current counter is converted to a static 15-minute history counter with an interval number 1, and a new current counter is started with an interval number 2.

This process continues for 24 hours, by the end of which, ninety six 15-minute history counters are created. After the creation of the ninety sixth 15-minute history counter, a new 24-hour counter is created along with a current counter that has an interval number 1. The 24-hour counter has the aggregated data of all the ninety six 15-minute history counters.

The 15-minute history counters that are created thereafter overwrite the existing set of ninety six 15-minute history counters, in the order they were created. Again, after the creation of the ninety sixth 15-minute history counter, the contents of the existing 24-hour counter are overwritten with new values. This entire process continues in a cyclic fashion.

**Note**

The performance history counters are reset if you reboot the Cisco ONS 15540 ESPx system, insert or remove the line card or SFP online, or change the encapsulation.

The performance history counters synchronize periodically from the primary CPU switch module to the standby CPU switch module enabling the system to preserve the performance data across a CPU switch module switchover.

**Note**

To enable or disable the syncing of the performance history counters to the standby CPU switch module, execute the **auto-sync counter interfaces** command.

Displaying Performance History Counters

To display the performance history counters, use the following EXEC commands:

Command	Purpose
show performance current [<i>interface</i>]	Displays the current counter for the specified interface ¹ .
show performance history [<i>interface</i>] [<i>interval number</i>]	Displays the 15-minute history counter for the specified interface and interval number ¹ .
show performance 24-hour [<i>interface</i>]	Displays the 24-hour counter for the specified interface ¹ .

1. If you do not specify the interface or interval number, the performance history counters for all interfaces or interval numbers are displayed.

To clear and reset all performance history counters, use the following EXEC command:

Command	Purpose
<code>clear performance history [interface]</code>	Clears the performance history counters for the specified interface.

Examples

The following example shows how to display the current counter for a tengigethernetphy interface:

```
Switch# show performance current tengigEthernetPhy 10/1
Current 15 minute performance register
-----
Interface      : TenGigEthernetPhy10/1
Interval Number : 55

Elapsed Time(seconds) : 660
Valid Time(seconds)   : 660

Code violation and running disparity error count : 0
TenGige Non CDL Pkt count : 0
CDL HEC error count      : 0
TenGige CDL idle Pkt count : 0
```

The following example shows how to display the 15-minute history counter for a tengigethernetphy interface:

```
Switch# show performance history tengigEthernetPhy 10/1 50
15 minute performance history register
-----
Interface      : TenGigEthernetPhy10/1
Interval Number : 50

Total Time(seconds) : 900
Valid Time(seconds) : 900

Code violation and running disparity error count : 0
TenGige Non CDL Pkt count : 0
CDL HEC error count      : 0
TenGige CDL idle Pkt count : 0
```

The following example shows how to display the 24-hour counter for a tengigethernetphy interface:

```
Switch# show performance 24-hour tengigEthernetPhy 10/1
24 hour performance register
-----
Interface      : TenGigEthernetPhy10/1

Total Time(seconds) : 86400
Valid Time(seconds) : 86400

Code violation and running disparity error count : 0
TenGige Non CDL Pkt count : 0
CDL HEC error count      : 0
TenGige CDL idle Pkt count : 0
```




Configuring PSM Interfaces

This chapter describes how to configure PSM (protection switch module) interfaces and patch connections on the Cisco ONS 15540 ESPx. This chapter includes the following sections:

- About the PSM, page 6-1
- Enabling Wdmsplit Interfaces, page 6-2
- Configuring Trunk Fiber Based Protection, page 6-3
- About Switchovers and Optical Power Thresholds, page 6-4
- Configuring Optical Power Thresholds, page 6-8
- Configuring Patch Connections, page 6-10
- Configuring Wdmsplit Interfaces in the Network Topology, page 6-11



Note

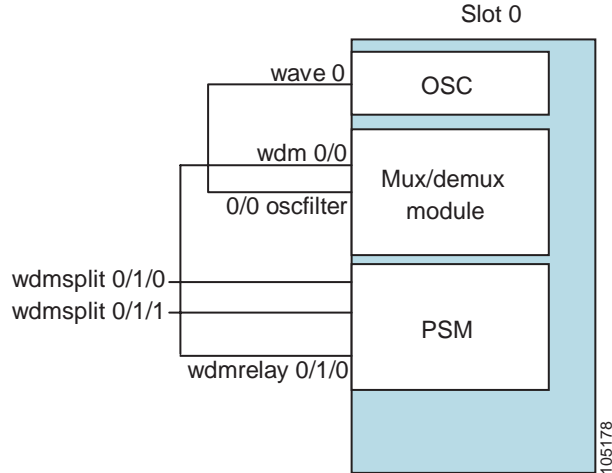
To ensure the installed Cisco IOS software supports your hardware and provides the software features you wish to use, see the “New and Changed Information” section on page xviii. Also refer to the “Hardware Supported” section and “Feature Set” section of the latest release notes for the Cisco ONS 15540 ESPx.

About the PSM

The PSM (protection switch module) provides trunk fiber protection for Cisco ONS 15540 ESPx systems configured in point-to-point topologies. The PSM sends the signal from a mux/demux module or a transponder module to both the west and east directions.

Figure 6-1 shows an example of PSM interfaces and their optical patch connections to a mux/demux module.

Figure 6-1 Optical Patch Connection Example Between a PSM and a Mux/Demux Module



Enabling Wdmsplit Interfaces

To enable the PSM wdmsplit interfaces, perform the following tasks, starting in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface wdmsplit slot/subcard/0 Switch(config-if)#	Specifies the west wdmsplit interface and enters interface configuration mode.
Step 2	Switch(config-if)# no shutdown	Enables the interface.
Step 3	Switch(config-if)# exit Switch(config)#	Returns to global configuration mode.
Step 4	Switch(config)# interface wdmsplit slot/subcard/1 Switch(config-if)#	Specifies the east wdmsplit interface and enters interface configuration mode.
Step 5	Switch(config-if)# no shutdown	Enables the interface.

Example

The following example shows how to enable wdmsplit interfaces:

```
Switch(config)# interface wdmsplit 0/0/0
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# interface wdmsplit 0/0/1
Switch(config-if)# no shutdown
```

Displaying Wdmsplit Interface Information

The following example shows how to display wdmsplit interface information.


```

Switch# show interface wdmsplit 0/1/0
WdmSplit0/1/0 is administratively down, line protocol is down
  Status                :Active
  Received power         :0.00 dBm (EF9)
  Threshold Value       :-22.00 dBm (8CE)

Optical threshold monitored for :Receive Power (in dBm)
Low alarm value         = -22.0 dBm (default)
Low Alarm Severity     = major
Low warning value       = -20.0 dBm (default)
Low Warning Severity   = not alarmed
High alarm value        = -2.0 dBm (default)
High Alarm Severity    = major
High warning value      = -4.0 dBm (default)
High Warning Severity  = not alarmed
Hardware is split wavelength_add_drop

```

Configuring Trunk Fiber Based Protection

To configure trunk fiber protection on the wdmsplit interfaces, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# redundancy Switch(config-red)#	Enters redundancy mode.
Step 2	Switch(config-red)# associate group <i>name</i> Switch(config-red-aps)#	Specifies an APS group name and enters APS configuration mode. Note The group name is case sensitive.
Step 3	Switch(config-red-aps)# aps working wdmsplit <i>slot/subcard/port</i>	Configures the working path interface.
Step 4	Switch(config-red-aps)# aps protection wdmsplit <i>slot/subcard/port</i>	Configures the protection path interface.
Step 5	Switch(config-red-aps)# aps message-channel { auto-select inband dcc ip osc } far-end <i>name</i>	Configures the name of the corresponding APS group on the other node in the topology.
Step 6	Switch(config-red-aps)# aps enable	Enables APS activity between the interfaces.

For more information on configuring APS and trunk fiber based protection, refer to Chapter 7, “Configuring APS.”

Examples

The following example shows how to configure trunk fiber protection:

```

Switch(config)# redundancy
Switch(config-red)# associate group psm-group
Switch(config-red-aps)# aps working wdmsplit 0/1/0
Switch(config-red-aps)# aps protection wdmsplit 0/1/1
Switch(config-red-aps)# aps message-channel ip far-end group-name psm-group ip-address 172.18.44.93
Switch(config-red-aps)# aps enable

```

Displaying Trunk Fiber Protection Configuration

To display the trunk fiber configuration, use the following EXEC command:

Command	Purpose
show aps { detail group name interface wavepatch slot/subcard/port }	Displays detailed APS configuration information for groups and interfaces.
	Note Group names are case sensitive.

Examples

The following example shows how to display the protocol encapsulation configuration of a wdm-split interface:

```
Switch# show aps group psm-group
APS Group psm-group :

architecture.: 1+1, remote prov: 1+1
span.....: end-to-end
prot. mode...: network side wdm splitter
direction...: prov: bi, current: bi, remote prov: bi
revertive....: no
aps state....: enabled (associated)
request timer: holddown: 5000 ms, max: 15000 ms, count 2
msg-channel...: ip (up), psm-group, 172.18.44.93
created.....: 22 hours, 11 minutes
auto-failover: disabled
transmit k1k2: sf-lp, 0, 0, 1+1, bi
receive k1k2: reverse-request, 0, 0, 1+1, bi
switched chan: 0
protection(0): WdmSplit0/0/1 (STANDBY - DOWN)
: channel request: sf-lp
: switchover count: 7
: last switchover: 18 minutes
working... (1): WdmSplit0/0/0 (ACTIVE - UP)
: channel request: no-request
: switchover count: 7
: last switchover: 18 minutes
```

About Switchovers and Optical Power Thresholds

The switchovers for trunk fiber protection on the PSM are controlled by an optical power threshold value set in the CLI. The value to set is determined by the characteristics of the point-to-point topology. The PSM supports the following types of point-to-point topologies:

- Unamplified
- Post-amplified
- Pre-amplified and post-amplified



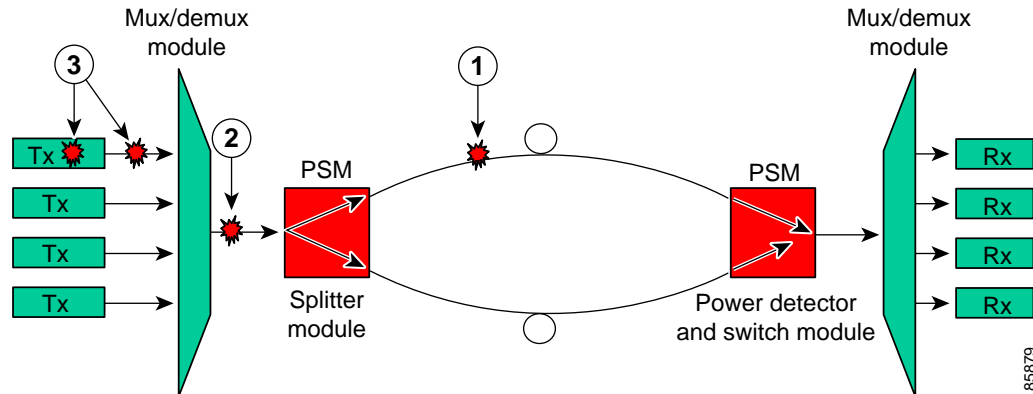
Note

Due to the cumulative effect of the noise from the EDFAs (erbium-doped fiber amplifiers), the PSM cannot support point-to-point topologies with more than two EDFAs on the trunk fiber. For topologies with three or more EDFAs on the trunk fiber, use splitter based protection.

Unamplified Topologies

A topology without amplification is the simplest case. Figure 6-2 shows an unamplified topology and the locations where failures can occur.

Figure 6-2 Point-to-Point Topology Without Amplification



1	Trunk fiber cut	3	Individual channel failures
2	Mux/demux module-to-PSM patch cable cut		



Note

The minimum channel power into the EDFA must be -15 dBm or higher.

The switching behavior for the failures is as follows:

- Trunk fiber cut

The receive power on the active path drops below the minimum detectable level (-31 dBm) and the PSM switches over to the standby path.
- Mux/demux module-to-PSM patch cable cut

In this case, the receive power on both the active and standby paths drops below the minimum detectable level. However, a switchover will occur if the auto-failover is enabled in the hardware. Since the system monitors the standby signal at 1 second intervals, the system might not detect the standby signal failure before the switchover occurs. After this switchover, no further switchovers occur.
- Individual channel failures

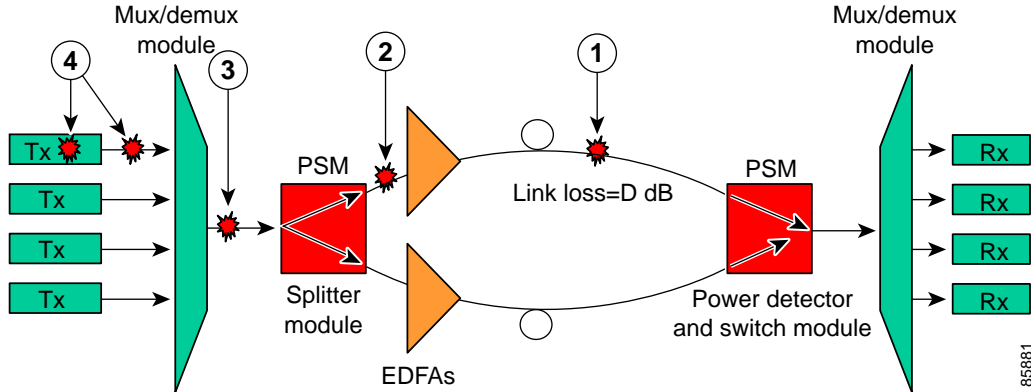
No switchover occurs because the change in the channel power is less than 15 dB.

The recommended low alarm threshold value for this topology is -28 dBm and the low warning threshold is at least -26 dBm.

Post-Amplified Topologies

Figure 6-3 shows an example topology with post-amplification and the locations where failures can occur.

Figure 6-3 Point-to-Point Topology with Post-Amplification



1	Trunk fiber cut	3	Mux/demux module-to-PSM patch cable cut
2	PSM-to-EDFA patch cable cut	4	Individual channel failures

**Note**

The minimum channel power into the EDFA must be -15 dBm or higher.

The switching behavior for the failures is as follows:

- Trunk fiber cut

The receive power on the active path drops below the minimum detectable level (-31 dBm) and the PSM switches over to the standby path.
- PSM-to-EDFA patch cable cut

The EDFA generates -9 dBm of noise on the active path so the PSM receives $(-9 - D)$ dBm signal power where D is the link loss between the EDFA and the PSM receiver. If the low alarm optical threshold is set correctly, the PSM switches over to the standby path.
- Mux/demux module-to-PSM patch cable cut

The EDFA generates -9 dBm of noise on both paths so the PSM receives $(-9 - D)$ dBm signal power where D is the link loss between the EDFA and the PSM receiver. If auto-failover is enabled and the low alarm optical threshold is set correctly, the PSM switches to the standby path before it detects that the standby path has also failed. No further switchovers occur.
- Individual channel failures

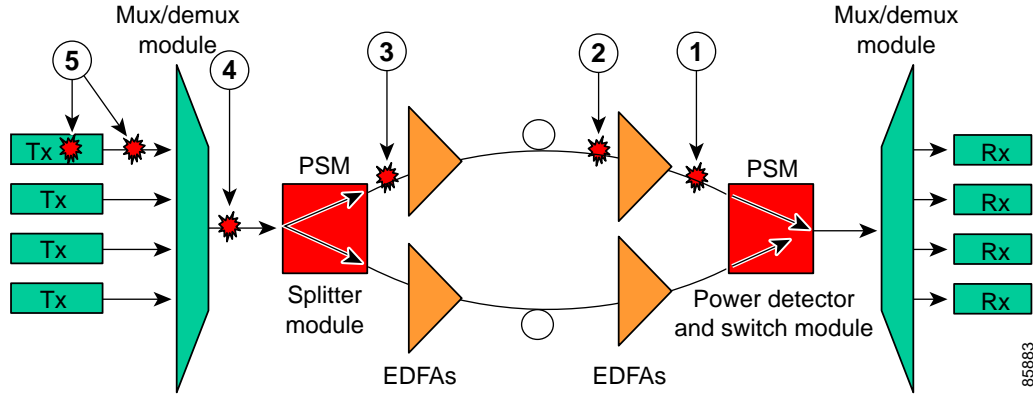
No switchover occurs because the change in the channel power is less than 15 dB.

The recommended value for the low alarm optical threshold is $(-6 - D)$ dBm and the low warning threshold is at least 2 dB higher.

Post-Amplified and Pre-amplified Topologies

Figure 6-4 shows an topology with post-amplification and preamplification and the locations where failures can occur.

Figure 6-4 Point-to-point Topology with Post-Amplification and Pre-Amplification



1	EDFA-to-PSM patch cable cut	4	Mux/demux module-to-PSM patch cable cut
2	Trunk fiber cut	5	Individual channel failures
3	PSM-to-EDFA patch cable cut		

Note

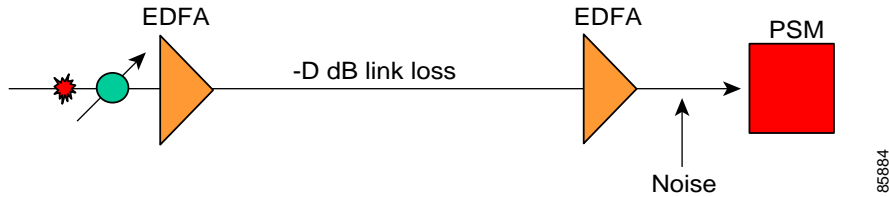
The minimum channel power into the EDFA must be -15 dBm or higher.

The switching behavior for the failures is as follows:

- EDFA-to-PSM patch cable cut
The receive power on the active path drops below the minimum detectable level (-31 dBm) and the PSM switches over to the standby path.
- Trunk fiber cut
The EDFA generates -9 dBm of noise so the PSM receives $(-9 - L)$ dBm signal power where L is the output attenuation from the EDFA. The PSM switches over to the standby path if the low alarm threshold is correctly configured.
- PSM-to-EDFA patch cable cut
The receive power drops, but not below the minimum detectable level because of the cumulative noise from the two EDFAs. The PSM switches over to the standby signal if the low alarm threshold is correctly configured.
- Mux/demux module-to-PSM patch cable cut
The receive power drops but not below the minimum detectable level because of the cumulative noise from the two EDFAs. If auto-failover is enabled, the PSM switches to the standby path before it detects that the standby path has also failed. No further switchovers occur.
- Individual channel failures
No switchover occurs because the change in the channel power is less than 15 dB.

Figure 6-5 shows an example topology and the locations where failures can occur.

Figure 6-5 Failure Scenario with Noise from Two EDFAs



You can calculate the noise using the following formula:

$$10 \text{ dB} * \log(10^{((-9)/10)} + 10^{((-9-D+17)/10)}) \text{ dB} - L \text{ dB}$$

where D is the link loss between the EDFAs and L is equal to 17 minus the configured gain on the EDFA closest to the PSM receiver.

The recommended value for the low alarm optical threshold is the calculated noise value plus 3 dBm.

Set the low warning threshold at least 2 dB higher.

Configuring Optical Power Thresholds

The optical power thresholds provide a means of monitoring the signal power received from the active trunk fiber path. Two types of thresholds are provided:

- Low alarm
- Low warning

When the low alarm threshold is crossed on the active path, the PSM switches over to the standby path. When either of the thresholds are crossed, the system sends messages to the console and generates traps, if traps are enabled.

To configure optical power thresholds for wdmsplit interfaces on a PSM, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface wdmsplit slot/subcard/0 Switch(config-if)#	Selects wdmsplit interface that carries traffic for the west direction and enters interface configuration mode.
Step 2	Switch(config-if)# optical threshold power receive {low high} {alarm warning} value [severity {critical major minor not alarmed not reported}]	Specifies the optical power threshold value in units of 0.1 dBm. The range is -280 to 0. The default values are as follows: Low alarm: -22 dBm Low warning: -20 dBm Alarm severity: major Warning severity: not alarmed
Step 3	Switch(config-if)# exit Switch(config)#	Returns to global configuration mode.

	Command	Purpose
Step 1	Switch(config)# interface wdmsplit slot/subcard/1 Switch(config-if)#	Selects the wdmsplit interface that carries traffic for the east direction and enters interface configuration mode.
Step 2	Switch(config-if)# optical threshold power receive {low high} {alarm warning} value [severity {critical major minor not alarmed not reported}]	Specifies the optical power threshold value in units of 0.1 dBm.

Examples

The following example shows how to configure optical power thresholds for wdmsplit interfaces on a PSM:

```
Switch(config)# interface wdmsplit 0/1/0
Switch(config-if)# optical threshold power receive low alarm -27
Switch(config-if)# optical threshold power receive low warning -25
Switch(config-if)# exit
Switch(config)# interface wdmsplit 0/1/1
Switch(config-if)# optical threshold power receive low alarm -26
Switch(config-if)# optical threshold power receive low warning -24
```

Displaying Optical Power Threshold Configuration

To display the optical power thresholds for a wdmsplit interface, use the following EXEC command:

Command	Purpose
show interfaces wdmsplit slot/subcard/port	Displays interface information.

Example

The following example shows how to display the optical threshold configuration for an interface:

```
Switch# show interfaces wdmsplit 0/1/0
WdmSplit0/1/0 is administratively down, line protocol is down
  Status                :Active
  Received power         :0.00 dBm (EF9)
  Threshold Value        :-22.00 dBm (8CE)

Optical threshold monitored for :Receive Power (in dBm)
Low alarm value         = -22.0 dBm (default)
Low Alarm Severity      = major
Low warning value       = -20.0 dBm (default)
Low Warning Severity    = not alarmed
Hardware is split wavelength_add_drop
```

Configuring Patch Connections

To configure patch connections between a PSM and a mux/demux module, use the following global configuration command:

Command	Purpose
<pre>patch wdm slot/subcard1 wdmrelay slot/subcard2/port</pre> or <pre>patch wdmrelay slot/subcard1/port wdm slot/subcard2</pre>	Configures the patch connection between a PSM and a mux/demux module.
<pre>patch wavepatch slot/subcard/port wdmrelay slot/subcard2/port</pre> or <pre>patch wdmrelay slot/subcard1/port wavepatch slot/subcard/port</pre>	Configures the patch connection between a PSM and a 2.5-Gbps transponder module or 10-GE transponder module. Note If you connect to a 2.5-Gbps transponder module, you must use IP to manage your network topology. If you connect to a 10-GE transponder module, you must use the ethernetdcc interface to manage your network topology.



Note

When the patch between a wdm interface and a wdmrelay interface is configured, CDP topology learning on the wdm interface is disabled.

Example

The following example shows how to configure the patch connections between a PSM and a mux/demux module:

```
Switch# configure terminal
Switch(config)# patch wdm 0/0 wdmrelay 0/1/0
```

Displaying Patch Connections

To display the patch connections, use the following privileged EXEC command:

Command	Purpose
<code>show patch [detail]</code>	Displays the patch connections.
<code>show interfaces { wdm slot/subcard1 wdmrelay slot/subcard2/port wavepatch slot/subcard/port }</code>	Displays the interface information.

Example

The following example shows the patch connections:

```
Switch# show patch
Patch Interface      Patch Interface      Type      Dir      Error
-----
Wdm0/0              WdmRelay0/1/0       USER      Both

Switch# show interfaces wdm0/0
```



```

Wdm0/0 is up, line protocol is up
  Patched Interface(s) :WdmRelay0/1/0
  Wdm Hw capability:N/A
  Num of Wavelengths Add/Dropped:5
  List of Wavelengths:0, 13, 14, 15, 16
  Hardware is wavelength_add_drop

```

Configuring Wdmsplit Interfaces in the Network Topology

The wdmsplit interfaces on a PSM do not support CDP and must be manually configured in the network topology.



Note

The patch connection between the PSM module and the mux/demux module or transponder module must be configured correctly. For more information on configuring the patches for these interfaces, see the “Configuring Patch Connections” section on page 6-10.



Note

When a patch connection between a mux/demux module and a PSM is configured, topology learning on the wdm interface is disabled.

To add wdmsplit interfaces to the network topology, perform the following steps on the wdmsplit interfaces on both the nodes in the point-to-point network topology, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface wdmsplit slot/subcard/0 Switch(config-if)#	Selects the west wdmsplit interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# topology neighbor {name <i>node-name</i> ip-address <i>node-ip-address</i> mac-address <i>node-mac-address</i> } {port {name <i>port-name</i> ip-address <i>port-ip-address</i> mac-address <i>port-mac-address</i> } }	Configures the network topology information for the neighboring node.
Step 3	Switch(config-if)# topology neighbor agent ip-address ip-address	Specifies the IP address of the network topology agent on the neighboring node.
Step 4	Switch(config-if)# exit Switch(config)#	Returns to interface configuration mode.
Step 5	Switch(config)# interface wdmsplit slot/subcard/1 Switch(config-if)#	Selects the east wdmsplit interface to configure and enters interface configuration mode.

	Command	Purpose
Step 6	Switch(config-if)# topology neighbor { name <i>node-name</i> ip-address <i>node-ip-address</i> mac-address <i>node-mac-address</i> } { port { name <i>port-name</i> ip-address <i>port-ip-address</i> mac-address <i>port-mac-address</i> } }	Configures the network topology information for the neighboring node.
Step 7	Switch(config-if)# topology neighbor agent ip-address <i>ip-address</i>	Specifies the IP address of the network topology agent on the neighboring node.

Example

The following example shows how to add wdmsplit interfaces to the network topology:

```
Switch(config)# interface wdmsplit 1/1/0
Switch(config-if)# topology neighbor name NodeB port name wdmsplit1/1/0
Switch(config-if)# topology neighbor agent ip-address 10.1.1.1
Switch(config-if)# exit
Switch(config)# interface wdmsplit 1/1/1
Switch(config-if)# topology neighbor name NodeB port name wdmsplit1/1/1
Switch(config-if)# topology neighbor agent ip-address 10.1.1.1
```

Displaying Topology Information for Wdmsplit Interfaces

To display the topology information for wdmsplit interfaces, use the following EXEC command:

Command	Purpose
show topology neighbor	Displays network topology information.

Example

The following example shows how to display the topology information:

```
Switch# show topology neighbor
Physical Topology:
```

Local Port	Neighbor Node	Neighbor Port	Link Dirn
-----	-----	-----	-----
WdmSplit0/1/0	PSM-2	wdms0/1/0	Both
WdmSplit0/1/1	PSM-2	wdms0/1/1	Both



Configuring APS

This chapter describes how to configure splitter protection and line card protection with APS (Automatic Protection Switching). This chapter contains the following sections:

- About APS, page 7-1
- About Splitter Protection, page 7-2
- Configuring Splitter Protection, page 7-3
- About Line Card Protection, page 7-6
- About Client Based Line Card Protection, page 7-6
- About Y-Cable Line Card Protection, page 7-7
- Configuring Y-Cable Based Line Card Protection, page 7-8
- About Trunk Fiber Based Protection, page 7-12
- Configuring Trunk Fiber Based Protection, page 7-14
- Configuring APS Group Attributes, page 7-15
- Switchovers and Lockouts, page 7-30



Note

To ensure the installed Cisco IOS software supports your hardware and provides the software features you wish to use, see the “New and Changed Information” section on page xviii. Also refer to the “Hardware Supported” section and “Feature Set” section of the latest release notes for the Cisco ONS 15540 ESPx.

About APS

APS provides protection against signal transmission failure. The Cisco ONS 15540 ESPx supports the following APS features:

- 1+1 path protection
- Splitter protection
- Line card protection
 - Client based
 - Y-cable based
- Trunk Fiber Based Protection

- Bidirectional and unidirectional path switching

The 1+1 path protection architecture transmits the client signal on both the working and protection paths.

**Note**

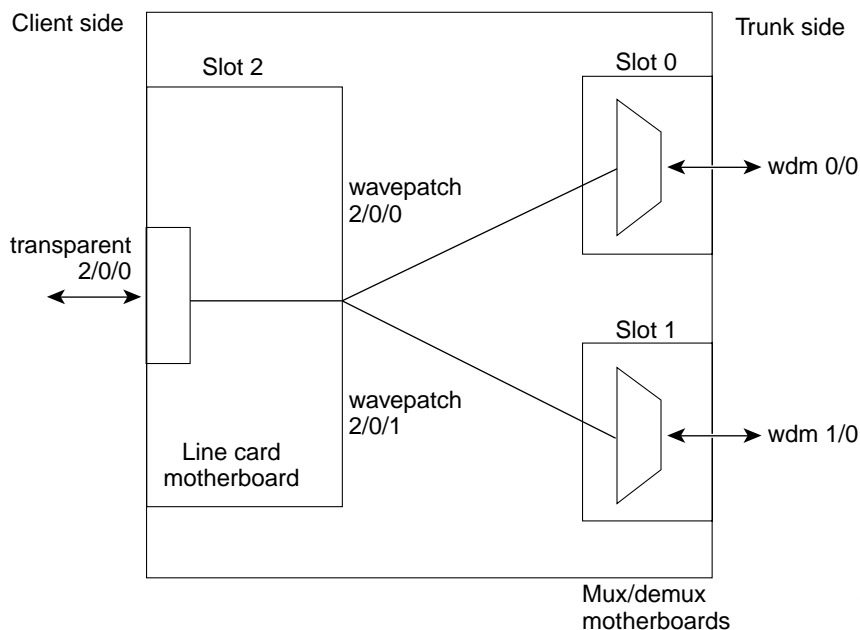
For an animated description of the APS implementation on the Cisco ONS 15540 ESPx, go to the following URL:

<http://www.cisco.com/mm/dyngraph/APS15540.html>

About Splitter Protection

Splitter protection on the Cisco ONS 15540 ESPx provides protection against facility failure, such as trunk fiber cuts, but not transponder module failures or client equipment failures. Splitter protection internally replicates the client optical signal received from the transponder module and transmits it to mux/demux modules in both slot 0 and slot 1 (see Figure 7-1).

Figure 7-1 Splitter Protection Scheme with 2.5-Gbps Transponder Module



On the trunk side, a fiber pair, with one receive fiber and one transmit fiber, connects to one mux/demux module in slot 0. Another trunk fiber pair connects to a mux/demux module in slot 1. The client signal is transmitted through both mux/demux modules to the trunk fiber pairs. A 2 x 2 switch on the line card fiber pairs receives both signals from the trunk fiber pairs and selects one as the active signal. When a signal failure is detected, the 2 x 2 switch switches over to the standby signal. The standby signal then becomes the active signal.

Considerations for Using Splitter Protection

The following considerations apply when considering the use of splitter protection:

- Each subcard position in the splitter protected line card motherboard corresponds to a specific filter interface on both of the mux/demux modules when using direct cross connections. If you are using a cross connect panel, channels can be cross connected between any subcard position on the line card motherboard and any filter interface on a mux/demux module.

For detailed information on cross connecting components, refer to the *Cisco ONS 15540 ESPx Planning Guide*.

- Splitter protection does not protect against failure in the transponder module, where the lasers are located. Splitter protection also does not protect against failure of the client equipment.

To protect against transponder module failure, use y-cable protection as described in the “About Line Card Protection” section on page 7-6 and the “Configuring Y-Cable Based Line Card Protection” section on page 7-8. To protect against both transponder module failure and client failure, implement protection on the client equipment instead.

- A system fully configured with 2.5-Gbps transponders can support 32 channels in splitter protection mode.
- A system fully configured with 10-GE transponder modules can support 16 channels in splitter protection mode.
- Splitter protection is nonrevertive. After correcting the problem that caused the signal failure and verifying the signal quality, you must manually switch the signal over to begin using the former working path. Use optical testing equipment to verify the signal quality.
- For interfaces with either Sysplex ETR or Sysplex CLO protocol encapsulation, configure bidirectional path switching to ensure proper functioning of the protocol.

For detailed information on shelf configuration rules, refer to the *Cisco ONS 15540 ESPx Planning Guide*.

Configuring Splitter Protection

The following steps describe the tasks required to configure splitter protection:

-
- Step 1** Determine the number of clients you need to support and which channels you will deploy to transport client data.
- Step 2** Ensure that the correct transponder modules are inserted in the line card motherboards in slots 2 through 5 and 8 through 11.
- Step 3** Ensure that the mux/demux modules needed to support the deployed channels are inserted in the correct subcards of the mux/demux motherboards.
- For each band of four or eight channels, you need two mux/demux modules that support the same channels.
- For detailed information on hardware configuration rules, refer to the *Cisco ONS 15540 ESPx Planning Guide*.
- Step 4** Ensure that the line card motherboards are correctly cross connected to the mux/demux modules and that the cabling configuration is correctly entered with the **patch** command on the CLI (command-line interface). For detailed information on the **patch** command, see the “About Patch Connections” section on page 4-21.

Ensure that the add/drop mux/demux modules are correctly interconnected with the external optical patch cables and that the cabling configuration is correctly entered with the **patch** command on the CLI. For detailed information on the **patch** command, see the “About Patch Connections” section on page 4-21.

Step 5 Configure APS from the CLI.



Caution

Laser safety control interrupts signal transmission with splitter protected configurations. If you configure the system with splitter protection and enable laser safety control, the transmit laser to the client shuts down when an open fiber occurs on one transport fiber and signal transmission to the client is interrupted.

To enable splitter protection, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# redundancy Switch(config-red)#	Enters redundancy configuration mode.
Step 2	Switch(config-red)# associate interface wavepatch */*/working-interface wavepatch */*/protection-interface [enable disable] or Switch(config-red)# associate interface wavepatch slot*/working-interface wavepatch slot*/protection-interface [enable disable]	Configures APS splitter protection mode on the entire chassis. The default state is disabled. or Configures APS splitter protection mode on the interfaces in a slot. The default state is disabled. Note The prompt stays in redundancy mode when the interface identifiers contain wildcards. To configure an individual interface pair, continue to the next step.
Step 3	Switch(config-red)# associate group name Switch(config-red-aps)#	Specifies an APS group name and enters APS configuration mode. Note The group name is case sensitive.
Step 4	Switch(config-red-aps)# aps disable	Disables APS activity between the interfaces. Note For newly created APS groups, APS activity is disabled by default.
Step 5	Switch(config-red-aps)# aps working wavepatch slot/subcard/port	Configures the working path interface.
Step 6	Switch(config-red-aps)# aps protection wavepatch slot/subcard/port	Configures the protection path interface.
Step 7	Switch(config-red-aps)# aps enable	Enables APS activity between the interfaces.

Examples

This example shows how to associate all the wavepatch interfaces in the shelf for splitter protection and enable APS activity.

```
Switch# configure terminal
Switch(config)# redundancy
```

```
Switch(config-red)# associate interface wavepatch */*/0 wavepatch */*/1 enable
Switch(config-red)#
```

This example shows how to associate all the wavepatch interfaces in slot 2 for splitter protection and enable APS activity.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate interface wavepatch 2/*/* wavepatch 2/*/*1 enable
Switch(config-red)#
```

This example shows how to associate wavepatch interfaces for the transponder module in slot 3 and subcard 0 for splitter protection and modify the default attribute settings.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group dallas1
Switch(config-red-aps)# aps working wavepatch 3/0/0
Switch(config-red-aps)# aps protection wavepatch 3/0/1
Switch(config-red-aps)# aps enable
```

Displaying the Splitter Protection Configuration

To display the splitter protection configuration, use the following EXEC commands:

Command	Purpose
show aps	Displays the APS configuration summary.
show aps {detail group <i>name</i> interface <i>wavepatch slot/subcard/port</i>}	Displays detailed APS configuration information for groups and interfaces.
	Note Group names are case sensitive.

Example

The following example shows how to display the APS splitter protection configuration:

```
Switch# show aps

AR : APS Role, Wk: Working, Pr: Protection
AS : APS State, Ac: Active, St: Standby
IS : Interface State, Up: Up, Dn: Down
MPL: Minimum Protection Level, SD: Signal Degrade, SF: Signal Failure
      LOL: Loss of Light, - not currently protected

Interface          AR AS IS MPL Redundant Intf      Group Name
~~~~~
Wavepatch5/3/0    Wk St Up   Wavepatch5/3/1    Seattle
Wavepatch5/3/1    Pr Ac Up LOL Wavepatch5/3/0    Seattle

Switch# show aps detail

APS Group Seattle :

architecture.: 1+1, remote prov: 1+1
span.....: end-to-end (network side splitter)
direction....: prov: uni, current: uni, remote prov: uni
revertive....: no
created.....: 14 hours, 54 minutes
aps state....: associated (enabled)
```

```
request timer: holddown: 5000 ms, max: 15000 ms, count 2
search-up int: min: 2 secs, max: 32 secs
switched chan: 1
channel ( 0): Wavepatch5/3/1 (ACTIVE - UP)
           : channel request: no-request
           : transmit request: do-not-revert
           : receive request: no-request
channel ( 1): Wavepatch5/3/0 (STANDBY - UP)
           : channel request: do-not-revert
           : switchover count: 1
           : last switchover: 14 hours, 54 minutes
```

About Line Card Protection

Line card protection on the Cisco ONS 15540 ESPx provides protection against both facility failures and line card failures. With line card protection, a duplicated signal is transmitted over ITU channels generated on separate line cards.

The Cisco ONS 15540 ESPx supports three types of line card protection:

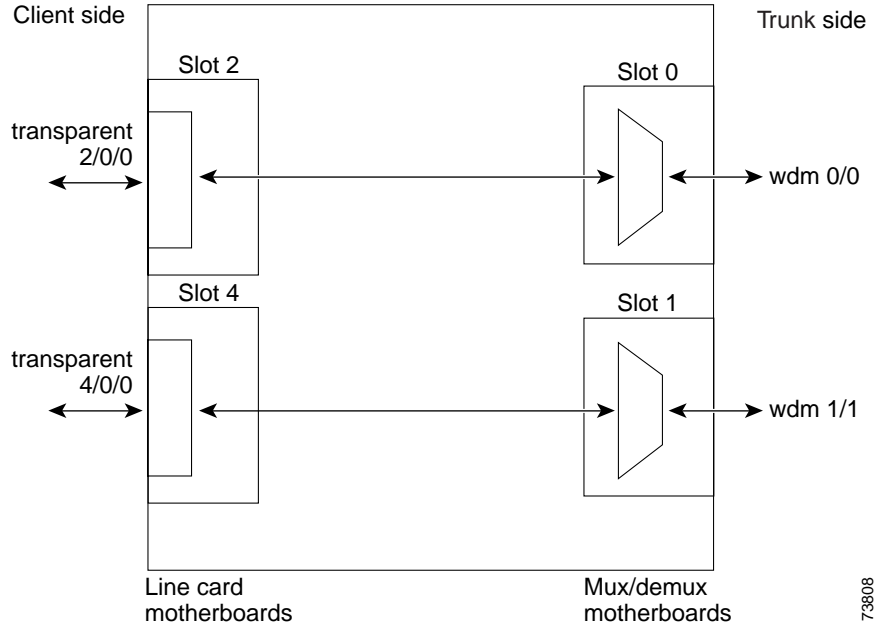
- Client based protection
- Y-cable protection
- Switch fabric based protection

About Client Based Line Card Protection

In client protection mode, both signals are transmitted to the client system. The client system decides which signal to use and when to switch over.

**Note**

Client protection does not require APS configuration on the Cisco ONS 15540 ESPx.

Figure 7-2 Line Card Protection Scheme with 2.5-Gbps Transponder Module

The Cisco ONS 15540 ESPx supports two types of line card protection, client protection and y-cable protection. In client protection mode, both signals are transmitted to the client system. The client system decides which signal to use and when to switch over.

**Note**

Client protection does not require APS configuration on the Cisco ONS 15540 ESPx.

With y-cable protection, the signal from only one of the transparent interfaces is transmitted to the client. The Cisco ONS 15540 ESPx turns on the laser at the active transparent interface, and turns off the laser on the standby transparent interface. At each receiver on the trunk side of the transponder module, the system monitors the optical signal power level. If the system detects a failure of the active signal when an acceptable signal exists on the standby transponder module, a switchover to the standby signal occurs by turning off the active transmitter at the client interface and turning on the standby transmitter.

About Y-Cable Line Card Protection

With y-cable protection, the client equipment sends only one signal to two transponder line cards using a y-cable to replicate the signal. The client equipment receives from only one transponder line card. The Cisco ONS 15540 ESPx turns on the laser at the active transparent interface, and turns off the laser on the standby transparent interface. At each receiver on the trunk side of the transponder line card, the system monitors the optical signal power level. If the system detects a failure of the active signal when an acceptable signal exists on the standby transponder line card, a switchover to the standby signal occurs by turning off the active transmitter at the client interface and turning on the standby transmitter.

Considerations for Using Y-Cable Based Line Card Protection

The following considerations apply when considering the use of line card protection:

- Cross connect the channels from the wavepatch interfaces on the line card motherboard to the filter interfaces on the mux/demux modules or the mux/demux motherboards. Each subcard position in an unprotected line card motherboard corresponds to a specific filter interface on a mux/demux module when using direct cross connections. If you are using a cross connect panel, channels can be cross connected between any subcard position on the line card motherboard and any filter interface on a mux/demux module.

For detailed information on cross connecting components, refer to the *Cisco ONS 15540 ESPx Planning Guide*.

- Y-cable line card protection does not protect against failures of the client equipment. To protect against client failures, ensure that protection is implemented on the client equipment itself.
- A fully provisioned single shelf of 2.5-Gbps transponder modules can support 16 channels in line card protection mode. A fully provisioned dual shelf of 2.5-Gbps transponder modules can support 32 channels in line card protection mode.
- A fully provisioned single shelf of 10-Gbps transponder modules can support 8 channels in line card protection mode. A fully provisioned dual shelf of 10-Gbps transponder modules can support 16 channels in line card protection mode.

For more information about dual shelf nodes, see Chapter 8, “Configuring Dual Shelf Nodes.”

- Y-cable line card protection supports revertive behavior. With revertive behavior, the signal automatically switches back to the working path after the signal failure has been corrected. The default behavior is nonrevertive.
- To simplify system management, terminate the client signal on two transponder modules of the same channel. In this way the client signal maps to the same WDM wavelength on both the working and protection paths.
- For interfaces with either Sysplex ETR or Sysplex CLO protocol encapsulation, configure bidirectional path switching to ensure proper functioning of the protocol.



Caution

Do not configure y-cable protection with Sysplex CLO, Sysplex ETR, or ISC compatibility protocol encapsulation, or with the OFC safety protocol.

Proper physical configuration of the system is critical to the operation of line card protection. For detailed information on shelf configuration rules, refer to the *Cisco ONS 15540 ESPx Planning Guide*.

Configuring Y-Cable Based Line Card Protection

The following is an overview of the tasks required to configure y-cable based line card protection:

-
- Step 1** Determine the number of clients you need to support and which channels you will deploy to transport the client data.
 - Step 2** Ensure that the mux/demux modules needed to support the channels are inserted in the correct subcards of the mux/demux motherboards; also ensure that the line card motherboards are cross connected to the mux/demux modules or mux/demux motherboards. (See the “Considerations for Using Y-Cable Based Line Card Protection” section on page 7-8.)

- Step 3** Ensure that the mux/demux modules are correctly interconnected with the external optical patch cables.
- Step 4** In order to ensure separate paths to the mux/demux modules, shut down the wavepatch interfaces if you are using splitter protected line card motherboards.
- Step 5** Configure the interfaces and the patch connections from the CLI.
- Step 6** Configure y-cable protection from the CLI.

Y-cable protection on the Cisco ONS 15540 ESPx requires configuration on the CLI. To configure y-cable protection, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# redundancy Switch(config-red)#	Enters redundancy configuration mode.
Step 2	Switch(config-red)# associate group name Switch(config-red-aps)#	Specifies an APS group name and enters APS configuration mode. The group name is case sensitive.
Step 3	Switch(config-red-aps)# aps disable	Disables APS activity between the interfaces. For newly associated pairs, APS activity is disabled by default.
Step 4	Switch(config-red-aps)# aps working { transparent slot/subcard/port tengigethernephy slot/subcard }	Configures the working path interface.
Step 5	Switch(config-red-aps)# aps protection { transparent slot/subcard/port tengigethernephy slot/subcard }	Configures the protection path interface.
Step 6	Switch(config-red-aps)# aps y-cable	Enables y-cable protection. The default state is no y-cable protection (disabled).
Step 7	Switch(config-red-aps)# aps enable	Enables APS activity between the interfaces.

**Note**

Configure both nodes that add and drop the channel with the same revertive behavior.

**Caution**

Do not configure y-cable protection with Sysplex CLO, Sysplex ETR, or ISC compatibility protocol encapsulation, or with the OFC safety protocol.

Example

This example shows how to associate two transparent interfaces for y-cable line card protection with revertive switchover behavior:

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group Yosemite
Switch(config-red-aps)# aps working transparent 3/0/0
Switch(config-red-aps)# aps protection transparent 5/0/0
Switch(config-red-aps)# aps y-cable
Switch(config-red-aps)# aps enable
```

Displaying the Y-Cable Protection Configuration

To display the y-cable protection configuration, use the following EXEC command:

Command	Purpose
<code>show aps</code>	Displays the APS configuration summary.
<code>show aps {detail group name interface {transparent slot/subcard/0 tengigetheretphy slot/subcard}}</code>	Displays detailed APS configuration information for interfaces and groups. Note Group names are case sensitive.

Examples

The following example shows how to display the y-cable protection for an APS group named Yosemite:

```
Switch# show aps
AR : APS Role, Wk: Working, Pr: Protection
AS : APS State, Ac: Active, St: Standby
IS : Interface State, Up: Up, Dn: Down
MPL: Minimum Protection Level, SD: Signal Degrade, SF: Signal Failure
      LOL: Loss of Light, - not currently protected

Interface          AR AS IS MPL Redundant Intf   Group Name
-----
Transparent2/3/0   Wk Ac Up SD   Transparent4/3/0 Yosemite
Transparent4/3/0   Pr St Up      Transparent2/3/0 Yosemite

Switch# show aps group Yosemite

APS Group Yosemite :
architecture.: 1+1, remote prov: 1+1
span.....: end-to-end (client side y-cable)
direction....: prov: uni, current: uni, remote prov: bi
revertive....: no
created.....: 14 hours, 53 minutes
aps state....: associated (enabled)
request timer: holddown: 5000 ms, max: 15000 ms, count 2
switched chan: 0
channel  ( 0): Transparent4/3/0 (STANDBY - UP), Wave4/3 (UP)
           : channel request: no-request
           : transmit request: no-request
           : receive request: no-request
channel  ( 1): Transparent2/3/0 (ACTIVE - UP), Wave2/3 (UP)
           : channel request: no-request
           : switchover count: 0
           : last switchover: never
```

The following example shows how to display the y-cable protection for an APS group on a 10-GE card, named y-protect:

```
Switch# show aps group y-protect

APS Group y-protect :

architecture.:1+1, remote prov:1+1
span.....:end-to-end
prot. mode...:client side y-cable
direction....:prov:uni, current:uni, remote prov:uni
```

```

revertive....:no
aps state....:enabled (associated)
request timer:holddown:5000 ms, max:15000 ms, count 2
msg-channel...:auto (up on cdl dcc)
created.....:2 minutes
auto-failover:enabled
transmit k1k2:no-request, 0, 0, 1+1, uni
receive k1k2:no-request, 0, 0, 1+1, uni
switched chan:0
protection(0):TenGigEthernetPhy9/1 (STANDBY - UP), WaveEthernetPhy9/1
(UP)
        :channel request:no-request
        :switchover count:0
        :last switchover:never
working... (1):TenGigEthernetPhy10/0 (ACTIVE - UP), WaveEthernetPhy10/0
(UP)
        :channel request:no-request
        :switchover count:0
        :last switchover:never

```

Configuring Splitter Protected Line Card Motherboards for Line Card Protection

Normally, you would use unprotected line card motherboards for line card protection configurations. However, you can use splitter protected line card motherboards instead by shutting down the wavepatch interfaces to one of the mux/demux motherboards.

To configure line card protection on splitter protected line card motherboards, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface wavepatch <i>slot/subcard/port</i> Switch(config-if)#	Selects the wavepatch interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# shutdown	Disables the wavepatch interface.
Step 3	Switch(config-if)# exit Switch(config)#	Returns to global configuration mode. Repeat Step 1 through Step 3 for one wavepatch interface per wavepatch pair on splitter protected line card motherboards.

Examples

For the following examples, assume that the line card motherboards shown in Figure 7-2 on page 7-7 have splitter protection.

The following example shows how to disable all wavepatch interfaces on the line card motherboard in slot 2 that connect to the mux/demux motherboard in slot 1:

```

Switch(config)# interface wavepatch 2/0/1
Switch(config-if)# shutdown
Switch(config-if)# exit
Switch(config)# interface wavepatch 2/1/1
Switch(config-if)# shutdown
Switch(config-if)# exit

```

```
Switch(config)# interface wavepatch 2/2/1
Switch(config-if)# shutdown
Switch(config-if)# exit
Switch(config)# interface wavepatch 2/3/1
Switch(config-if)# shutdown
Switch(config-if)# exit
Switch(config)#
```

The following example shows how to disable all wavepatch interfaces on the line card motherboard in slot 4 that connect to the mux/demux motherboard in slot 0:

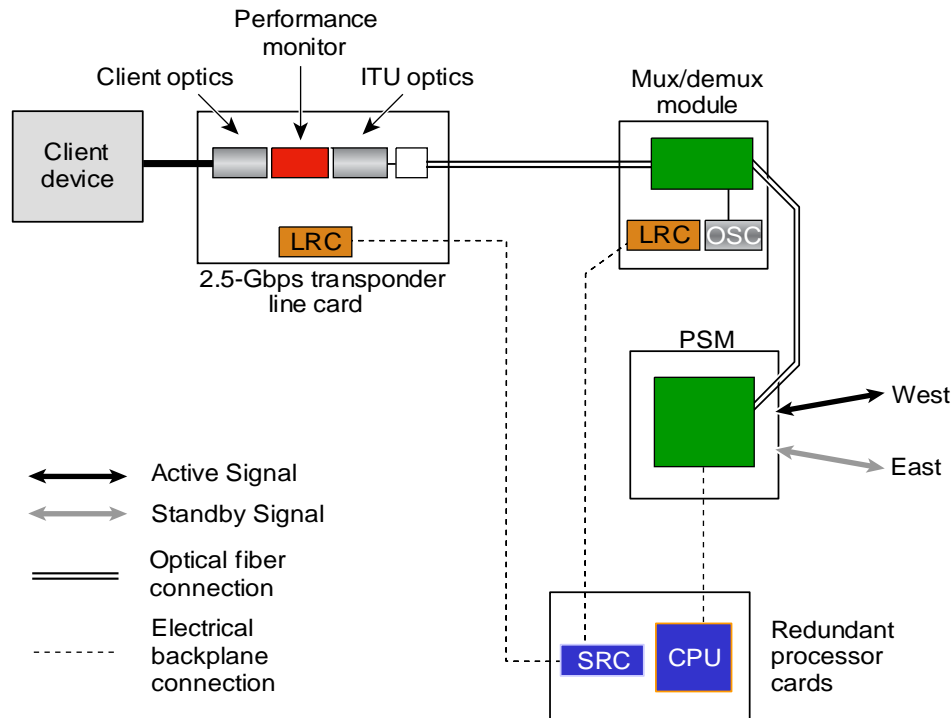
```
Switch(config)# interface wavepatch 4/0/0
Switch(config-if)# shutdown
Switch(config-if)# exit
Switch(config)# interface wavepatch 4/1/0
Switch(config-if)# shutdown
Switch(config-if)# exit
Switch(config)# interface wavepatch 4/2/0
Switch(config-if)# shutdown
Switch(config-if)# exit
Switch(config)# interface wavepatch 4/3/0
Switch(config-if)# shutdown
Switch(config-if)# exit
Switch(config)#
```

About Trunk Fiber Based Protection

The PSM (protection switch module) provides trunk fiber based protection for Cisco ONS 15540 ESPx systems configured in point-to-point topologies. This type of protection only provides protection against trunk fiber cuts, not specific channel failure as provided by splitter and line card based schemes. However, this protection scheme allows for much simpler shelf configurations in topologies where per channel protection is not required.

Figure 7-3 shows trunk fiber based protection configured with a transponder line card.

Figure 7-3 Trunk Fiber Based Protection Scheme



Considerations for Using Trunk Fiber Based Protection

The following considerations apply when using trunk fiber based protection:

- Trunk fiber based protection does not protect against failures on the shelf itself or the client equipment. To protect against these failures, line card protection should be implemented on the client equipment itself.
- The APS software that supports trunk fiber based protection can be configured as revertive or nonrevertive. After a switchover, the active traffic can be put back on the previously failed working fiber, once the fault has been remedied, either automatically (revertive) or through manual intervention (nonrevertive).
- Use PSMs only in point-to-point topologies.
- The shelves connected to the trunk fiber must use a PSM.

Configuring Trunk Fiber Based Protection

To configure trunk fiber based protection on the PSMs, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# redundancy Switch(config-red)#	Enters redundancy mode.
Step 2	Switch(config-red)# associate group name Switch(config-red-aps)#	Specifies an APS group name and enters APS configuration mode. Note The group name is case sensitive.
Step 3	Switch(config-red-aps)# aps working wdmsplit slot/subcard	Configures the working path interface.
Step 4	Switch(config-red-aps)# aps protection wdmsplit slot/subcard	Configures the protection path interface.
Step 5	Switch(config-red-aps)# aps message-channel {auto-select inband dcc ip osc} far-end name	Configures the name of the corresponding APS group on the other node in the topology.
Step 6	Switch(config-red-aps)# aps enable	Enables APS activity between the interfaces.

Examples

The following example shows how to configure trunk fiber protection:

```
Switch(config)# redundancy
Switch(config-red)# associate group psm-group
Switch(config-red-aps)# aps working wdmsplit 0/1/0
Switch(config-red-aps)# aps protection wdmsplit 0/1/1
Switch(config-red-aps)# aps message-channel ip far-end group-name psm-group ip-address
172.18.44.93
Switch(config-red-aps)# aps enable
```

Displaying Trunk Fiber Protection Configuration

To display the trunk fiber configuration, use the following EXEC command:

Command	Purpose
show aps {detail group name interface wavepatch slot/subcard/port}	Displays detailed APS configuration information for groups and interfaces. Note Group names are case sensitive.

Examples

The following example shows how to display the protocol encapsulation configuration of a wdmsplit interface:

```
Switch# show aps group psm-group
APS Group psm-group :

architecture.: 1+1, remote prov: 1+1
span.....: end-to-end
```



```

prot. mode...: network side wdm splitter
direction...: prov: bi, current: bi, remote prov: bi
revertive....: no
aps state....: enabled (associated)
request timer: holddown: 5000 ms, max: 15000 ms, count 2
msg-channel...: ip (up), psm-group, 172.18.44.93
created.....: 22 hours, 11 minutes
auto-failover: disabled
transmit k1k2: sf-lp, 0, 0, 1+1, bi
receive k1k2: reverse-request, 0, 0, 1+1, bi
switched chan: 0
protection(0): WdmSplit0/0/1 (STANDBY - DOWN)
                : channel request: sf-lp
                : switchover count: 7
                : last switchover: 18 minutes
working... (1): WdmSplit0/0/0 (ACTIVE - UP)
                : channel request: no-request
                : switchover count: 7
                : last switchover: 18 minutes

```

Configuring APS Group Attributes

This section describes APS group attributes and how to configure them.

Configuring Revertive Switching

The Cisco ONS 15540 ESPx supports revertive switching for y-cable and trunk fiber protection. When revertive switching is configured, the system automatically switches back from the protection interface to the working interface. This automatic switchover occurs after the condition that caused the switchover to the protection interface is resolved and the switchover-enable timer has expired.

To configure revertive switching, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# redundancy Switch(config-red)#	Enters redundancy configuration mode.
Step 2	Switch(config-red)# associate group name Switch(config-red-aps)#	Selects the interfaces to associate and enters APS configuration mode. Note The group name is case sensitive.
Step 3	Switch(config-red-aps)# aps disable	Disables APS activity between the interfaces.
Step 4	Switch(config-red-aps)# aps timer wait-to-restore seconds	Modifies the interval for the wait-to-restore timer. If revertive protection is configured and a switchover has occurred, the system will wait this amount of time before switching back to the functioning working path. The default value is 300 seconds. (Optional)
Step 5	Switch(config-red-aps)# aps revertive	Enables revertive switchover behavior. The default behavior is nonrevertive.
Step 6	Switch(config-red-aps)# aps enable	Enables APS activity between the interfaces.

Example

The following example shows how to configure revertive switching for a y-cable protected APS group:

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group blue
Switch(config-red-aps)# aps working transparent 4/0/0
Switch(config-red-aps)# aps protection transparent 8/0/0
Switch(config-red-aps)# aps y-cable
Switch(config-red-aps)# aps revertive
Switch(config-red-aps)# aps enable
```

Displaying the Revertive Switching Configuration

To display the revertive switching configuration, use the following EXEC command:

Command	Purpose
show aps [detail group name interface { transparent slot/subcard/0 wdm-split slot/subcard/slot }]	Displays the APS configuration for interfaces and groups.
	Note Group names are case sensitive.

Example

The following example shows how to display the path switching configuration for an APS group named blue:

```
Switch# show aps group blue
```

```
APS Group blue:
```

```
architecture.: 1+1, remote prov: 1+1
span.....: end-to-end
prot. mode...: client side y-cable
direction...: prov: uni, current: uni, remote prov: uni
→ revertive...: yes, wtr: 300 secs (not running)
aps state...: enabled (associated)
request timer: holddown: 5000 ms, max: 15000 ms, count 2
msg-channel..: auto (up on osc)
created.....: 4 days, 23 hours, 16 minutes
auto-failover: enabled
transmit k1k2: no-request, 0, 0, 1+1, uni
receive k1k2: no-request, 0, 0, 1+1, uni
switched chan: 0
protection(0): Transparent8/0/0 (STANDBY - UP), Wave8/0 (UP)
                : channel request: no-request
                : switchover count: 2
                : last switchover: 3 days, 23 hours, 16 minutes
working... (1): Transparent4/0/0 (ACTIVE - UP), Wave4/0 (UP)
                : channel request: no-request
                : switchover count: 1
                : last switchover: 4 days, 53 minutes
```

About Path Switching

The Cisco ONS 15540 ESPx supports per-channel unidirectional and bidirectional 1+1 path switching. When a signal is protected and the signal fails, or in some cases degrades, on the active path, the system automatically switches from the active network path to the standby network path.

Signal failures can be total loss of light caused by laser failures, by fiber cuts between the Cisco ONS 15540 ESPx and the client equipment, or by other equipment failure. Loss of light failures cause switchovers for both splitter protected and y-cable protected signals.

For y-cable protected signals, you can also configure alarm thresholds to cause a switchover when the signal error rate reaches an unacceptable level. For information about configuring alarm thresholds, see the “Configuring Alarm Thresholds” section on page 4-9.



Note

Both interfaces on both nodes must be configured with alarm thresholds for signal error rate switchovers to occur.

The Cisco ONS 15540 ESPx implements path switching using an APS channel protocol over the in-band message channel, the OSC (optical supervisory channel) on the protection path, or the IP management connection.



Note

Bidirectional path switching operates only on Cisco ONS 15540 ESPx networks that have the OSC or the in-band message channel, or send the APS message over the IP management connection. You must also configure the patch connection between the OSC and the mux/demux motherboard if you are using the OSC for APS messages.

Figure 7-4 shows a simple point-to-point configuration with splitter protection. The configured working path carries the active signal, and the configured protection path carries the standby signal.

Figure 7-4 Active and Standby Path Configuration Example

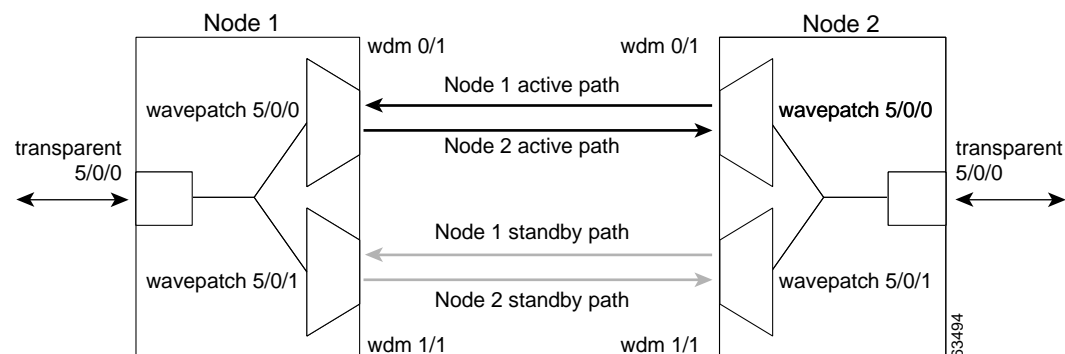


Figure 7-5 shows the behavior of unidirectional path switching when a loss of signal occurs. For the two node example network, unidirectional path switching operates as follows:

- Node 2 sends the channel signal over both the active and standby paths.
- Node 1 receives both signals and selects the signal on the active path.
- Node 1 detects a loss of signal light on its active path and switches over to the standby path.

- Node 2 does not switch over and continues to use its original active path.

Now the nodes are communicating along different paths.

Figure 7-5 Unidirectional Path Switching Example

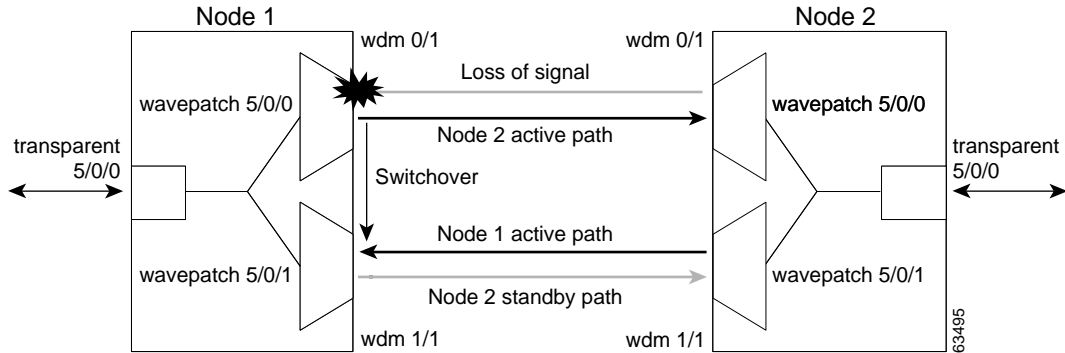
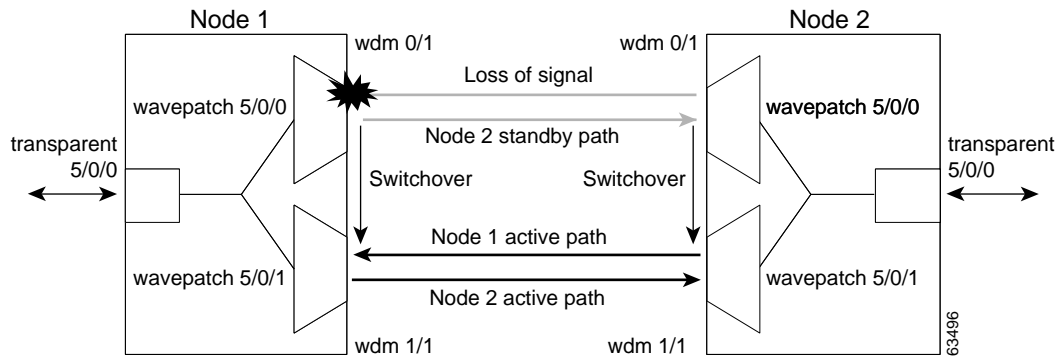


Figure 7-6 shows the behavior of bidirectional path switching when a loss of signal occurs. For the two node example network, bidirectional path switching operates as follows:

- Node 2 sends the channel signal over both the active and standby paths.
- Node 1 receives both signals and selects the signal on the active path.
- Node 1 detects a loss of signal light on its active path and switches over to the standby path.
- Node 1 sends an APS switchover message to node 2 on the protection path.
- Node 2 switches from the active path to the standby path.

Both node 1 and node 2 communicate on the same path.

Figure 7-6 Bidirectional Path Switching Overview



Configuring Path Switching

To configure unidirectional or bidirectional path switching, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# redundancy Switch(config-red)#	Enters redundancy configuration mode.
Step 2	Switch(config-red)# associate group name Switch(config-red-aps)#	Selects the interfaces to associate and enters APS configuration mode. Note The group name is case sensitive.
Step 3	Switch(config-red-aps)# aps disable	Disables APS activity between the interfaces. Note For newly associated pairs, APS activity is disabled by default.
Step 4	Switch(config-red-aps)# aps direction { unidirectional bidirectional }	Specifies the type of path switching. The default behavior is unidirectional.
Step 5	Switch(config-red-aps)# aps working { transparent slot/subcard/0 wavepatch slot/subcard/port tengigethernetphy slot/subcard wdmsplit slot/subcard/port }	Configures the working path interface.
Step 6	Switch(config-red-aps)# aps protection { transparent slot/subcard/0 wavepatch slot/subcard/port tengigethernetphy slot/subcard wdmsplit slot/subcard/port }	Configures the protection path interface.
Step 7	Switch(config-red-aps)# aps timer oscp holddown milliseconds count number	Changes the APS channel protocol holddown timer and message count values. The default is 5000 milliseconds and a count of 2
Step 8	Switch(config-red-aps)# aps timer oscp max-interval seconds	Changes the APS channel protocol maximum interval timer for waiting for a message. The default is 15 seconds. Repeat Step 1 through Step 8 on the corresponding transparent interface on the other node that adds and drops, or terminates, the channel.
Step 9	Switch(config-red-aps)# aps enable	Enables APS activity between the interfaces.



Note

Both nodes in the network that add and drop the channel must have the same APS configuration. Specifically, both must have the same path switching behavior, and working and protection paths.



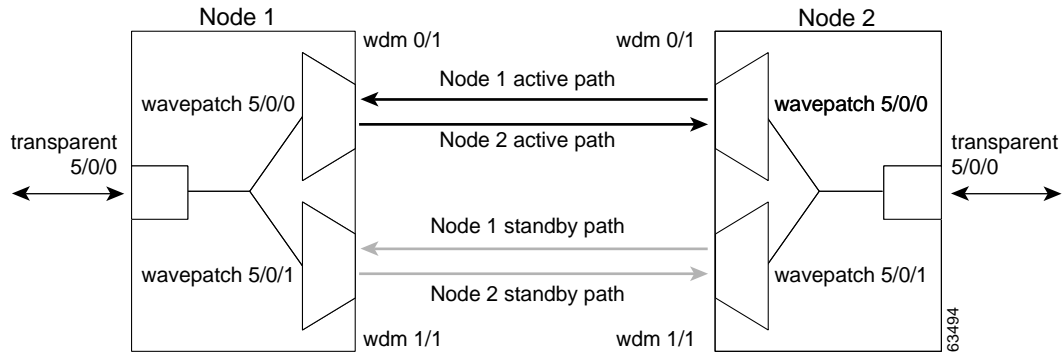
Note

For interfaces with either Sysplex ETR or Sysplex CLO protocol encapsulation, configure bidirectional path switching to ensure proper functioning of the protocol.

Examples

Figure 7-7 shows the active and standby paths between node 1 and node 2 with splitter protection.

Figure 7-7 Bidirectional Path Switching Example with Splitter Protection



The following example shows how to configure one channel in the example network for bidirectional path switching using the default working and protection path interfaces:

```

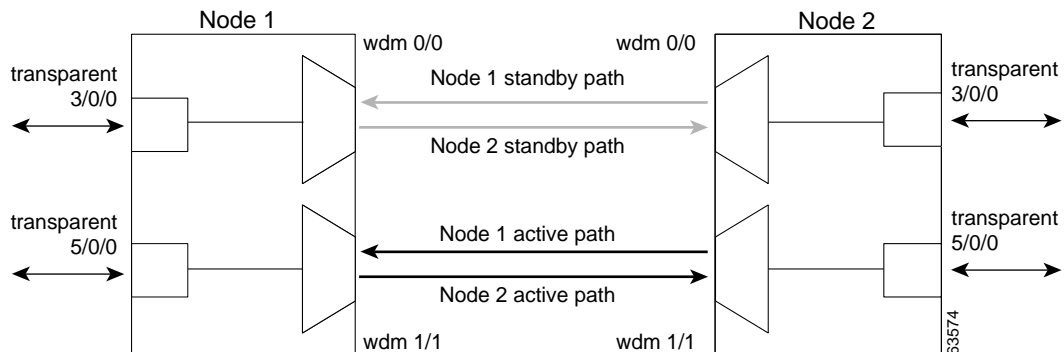
Node1# configure terminal
Node1(config)# redundancy
Node1(config-red)# associate group red
Node1(config-red-aps)# aps working wavepatch 5/0/0
Node1(config-red-aps)# aps protection wavepatch 5/0/1
Node1(config-red-aps)# aps bidirectional
Node1(config-red-aps)# aps enable

Node2# configure terminal
Node2(config)# redundancy
Node2(config-red)# associate group blue
Node2(config-red-aps)# aps working wavepatch 5/0/0
Node2(config-red-aps)# aps protection wavepatch 5/0/1
Node2(config-red-aps)# aps bidirectional
Node2(config-red-aps)# aps enable

```

Figure 7-8 shows the active and standby paths between node 1 and node 2 with y-cable protection.

Figure 7-8 Bidirectional Path Switching Example with Y-Cable Protection



The following example shows how to configure one channel in the example network for bidirectional path switching and configure the working and protection path interfaces:

```

Node1# configure terminal

```

```

Node1(config)# redundancy
Node1(config-red)# associate group alpha
Node1(config-red-aps)# aps working transparent 5/0/0
Node1(config-red-aps)# aps protection transparent 3/0/0
Node1(config-red-aps)# aps direction bidirectional
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps enable

Node2# configure terminal
Node2(config)# redundancy
Node2(config-red)# associate group alpha
Node2(config-red-aps)# aps working transparent 5/0/0
Node2(config-red-aps)# aps protection transparent 3/0/0
Node2(config-red-aps)# aps direction bidirectional
Node2(config-red-aps)# aps y-cable
Node2(config-red-aps)# aps enable

```

Changing the Path Switching Direction for Y-Cable Protection

To change the path switching direction for a y-cable protection configuration, use the following commands:

	Command	Purpose
Step 1	Switch# show aps group <i>name</i>	Displays the current standby interface in the APS group information.
Step 2	Switch# configure terminal Switch(config)#	Enters global configuration mode.
Step 3	Switch(config)# interface transparent <i>slot/subcard/0</i> Switch(config-if)#	Enters interface configuration mode for the standby interface.
Step 4	Switch(config-if)# shutdown	Disables the interface.
Step 5	Switch(config-if)# exit Switch(config)#	Exits interface configuration mode.
Step 6	Switch(config)# redundancy Switch(config-red)#	Enters redundancy configuration mode.
Step 7	Switch(config-red)# associate group <i>name</i> Switch(config-red-aps)#	Selects the interfaces to associate and enters APS configuration mode. Note The group name is case sensitive.
Step 8	Switch(config-red-aps)# aps disable	Disables APS activity between the interfaces. Note For newly associated pairs, APS activity is disabled by default.
Step 9	Switch(config-red-aps)# aps direction { unidirectional bidirectional }	Specifies the new path switching operation.
Step 10	Switch(config-red-aps)# aps enable	Enables APS activity between the interfaces.
Step 11	Switch(config-red-aps)# exit Switch(config)#	Exits APS configuration mode.

	Command	Purpose
Step 12	Switch(config-red)# exit Switch(config)#	Exits redundancy configuration mode.
Step 13	Switch(config)# interface transparent slot/subcard/0 Switch(config-if)#	Enters interface configuration mode for the standby interface.
Step 14	Switch(config-if)# no shutdown	Disables the interface.
Step 15	Switch(config-if)# end Switch#	Returns to privileged EXEC mode. Repeat Step 1 through Step 15 on the corresponding transparent interface on the other node that adds and drops, or terminates, the channel.

Example

The following example shows how to change the path switching operation for a y-cable APS group from unidirectional to bidirectional:

```

Node1# show aps group Denver

APS Group Denver :

architecture.: 1+1, remote prov: 1+1
span.....: end-to-end (client side y-cable)
direction...: prov: uni, current: uni, remote prov: uni
revertive...: no
created.....: 14 hours, 53 minutes
aps state...: associated (enabled)
request timer: holddown: 5000 ms, max: 15000 ms, count 2
switched chan: 0
→ channel ( 0): Transparent4/3/0 (STANDBY - UP), Wave4/3 (UP)
   : channel request: no-request
   : transmit request: no-request
   : receive request: no-request
channel ( 1): Transparent2/3/0 (ACTIVE - UP), Wave2/3 (UP)
   : channel request: no-request
   : switchover count: 0
   : last switchover: never

Node1# configure terminal
Node1(config)# interface transparent 4/3/0
Node1(config-if)# shutdown
Node1(config-if)# exit
Node1(config)# redundancy
Node1(config-red)# associate group Denver
Node1(config-red-aps)# aps disable
Node1(config-red-aps)# aps direction bidirectional
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# exit
Node1(config)# interface transparent 4/3/0
Node1(config-if)# no shutdown
Node1(config-if)# end
Node1#

Node2# show aps group Denver

APS Group Denver :
```



```

architecture.: 1+1, remote prov: 1+1
span.....: end-to-end (client side y-cable)
direction....: prov: uni, current: uni, remote prov: bi
revertive....: no
created.....: 14 hours, 53 minutes
aps state....: associated (enabled)
request timer: holddown: 5000 ms, max: 15000 ms, count 2
switched chan: 0
→ channel ( 0): Transparent4/3/0 (STANDBY - UP), Wave4/3 (UP)
      : channel request: no-request
      : transmit request: no-request
      : receive request: no-request
channel ( 1): Transparent2/3/0 (ACTIVE - UP), Wave2/3 (UP)
      : channel request: no-request
      : switchover count: 0
      : last switchover: never

Node2# configure terminal
Node2(config)# interface transparent 4/3/0
Node2(config-if)# shutdown
Node2(config-if)# exit
Node2(config)# redundancy
Node2(config-red)# associate group Denver
Node2(config-red-aps)# aps disable
Node2(config-red-aps)# aps direction bidirectional
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# exit
Node2(config-red)# exit
Node2(config)# interface transparent 4/3/0
Node2(config-if)# no shutdown
Node2(config-if)# end
Node2#

```

Displaying the Path Switching Configuration

To display the path switching configuration, use the following EXEC command:

Command	Purpose
show aps [detail group name interface { transparent slot/subcard/0 wavepatch slot/subcard/port tengigethernetphy slot/subcard wdmsplit slot/subcard/port }]	Displays the APS configuration for interfaces and groups. Note Group names are case sensitive.

Example

The following example shows how to display the path switching configuration for an APS group named blue:

```

Switch# show aps group blue

APS Group blue:

architecture.: 1+1, remote prov: 1+1
span.....: end-to-end
→ direction....: prov: bi, current: bi, remote prov: bi
revertive....: no
created.....: 26 minutes
aps state....: associated

```

```

request timer: holddown: 5000 ms, max: 15 secs, count 2
switched chan: 0
channel ( 0): Wavepatch8/0/1 (STANDBY - UP)
           : channel request: no-request
           : transmit request: no-request
           : receive request: no-request
channel ( 1): Wavepatch8/0/0 (ACTIVE - UP)
           : channel request: no-request
           : switchover count: 0
           : last switchover: never

```

Configuring the Switchover-Enable Timer

The switchover-enable timer on the Cisco ONS 15540 ESPx prevents any automatic switchover from the protection path to the working path until it has expired. When it expires, switchovers occur only if there is no fault on the working path and there is no overriding switchover request in effect.

To configure the switchover-enable timer, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# redundancy Switch(config-red)#	Enters redundancy configuration mode.
Step 2	Switch(config-red)# associate group <i>name</i> Switch(config-red-aps)#	Selects the interfaces to associate and enters APS configuration mode. Note The group name is case sensitive.
Step 3	Switch(config-red-aps)# aps disable	Disables the APS group.
Step 4	Switch(config-red-aps)# aps timer switchover-enable min-interval <i>seconds</i>	Modifies the timer that controls the check on the status of the working path. The default is 3 seconds.
Step 5	Switch(config-red-aps)# aps enable	Enables the APS group.

Example

The following example shows how to configure the minimum interval value for the switchover-enable timer for an APS group.

```

Switch(config)# redundancy
Switch(config-red)# associate group yc
Switch(config-red-aps)# aps disable
Switch(config-red-aps)# aps timer switchover-enable min-interval 10
Switch(config-red-aps)# aps enable

```

Displaying the Switchover-Enable Timer Configuration

To display the switchover-enable timer configuration, use the following EXEC command:

Command	Purpose
show aps [detail group name interface { transparent slot/subcard/0 wavepatch slot/subcard/port tengigethernetphy slot/subcard wdmsplit slot/subcard/port }]	Displays the APS configuration for interfaces and groups. Note Group names are case sensitive.

Example

The following example shows how to display the switchover-enable timer configuration for an APS group:

```
Switch# show running-config
Building configuration...

Current configuration : 3403 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname M1
!
redundancy
  keepalive-timer 4000
  keepalive-threshold 12
  associate group yc
    aps working Transparent8/0/0
    aps protection Transparent8/3/0
    aps y-cable
    aps enable
→   aps timer switchover-enable min-interval 10

<Information deleted.>
```

Configuring the Wait-to-Restore Timer

The wait-to-restore timer on the Cisco ONS 15540 ESPx prevents oscillations when revertive switching is enabled for y-cable line card protection configurations. If the preferred working signal in a y-cable line card protection configuration is unstable, the wait-to-restore timer prevents possible data loss that could result from frequent switchovers.

To configure the wait-to-restore timer, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# redundancy Switch(config-red)#	Enters redundancy configuration mode.
Step 2	Switch(config-red)# associate group <i>name</i> Switch(config-red-aps)#	Selects the interfaces to associate and enters APS configuration mode. Note The group name is case sensitive.
Step 3	Switch(config-red-aps)# aps disable	Disables the APS group.
Step 4	Switch(config-red-aps)# aps timer wait-to-restore <i>seconds</i>	Modifies the timer that controls the check on the status of the working path. The default is 300 seconds.
Step 5	Switch(config-red-aps)# aps enable	Enables the APS group.

Example

The following example shows how to configure the wait-to-restore timer value for an APS group.

```
Switch(config)# redundancy
Switch(config-red)# associate group blue
Switch(config-red-aps)# aps disable
Switch(config-red-aps)# aps timer wait-to-restore 240
Switch(config-red-aps)# aps enable
```

Displaying the Wait-to-Restore Timer Configuration

To display the wait-to-restore timer configuration, use the following EXEC command:

Command	Purpose
show aps [detail group <i>name</i> interface { transparent <i>slot/subcard/0</i> wavepatch <i>slot/subcard/port</i> tengigethernetphy <i>slot/subcard</i> wdmsplit <i>slot/subcard/port</i> }]	Displays the APS configuration for interfaces and groups. Note Group names are case sensitive.

Example

The following example shows how to display the wait-to-restore timer configuration for an APS group named blue:

```
Switch# show aps group blue

APS Group blue:

architecture.: 1+1, remote prov: unknown
span.....: end-to-end
prot. mode...: client side y-cable
direction...: prov: uni, current: uni, remote prov: unknown
→ revertive...: yes, wtr: 240 secs (running - 232 secs left)
aps state...: enabled (associated)
request timer: holddown: 5000 ms, max: 15000 ms, count 2
msg-channel..: auto (down)
created.....: 4 days, 25 minutes
```

```

auto-failover: enabled
transmit k1k2: wait-to-restore, 1, 1, 1+1, uni
receive k1k2: no-request, 0, 0, unknown, unknown
switched chan: 1
protection(0): Transparent8/3/0 (ACTIVE - UP), Wave8/3 (UP)
                 : channel request: no-request
                 : switchover count: 0
                 : last switchover: never
working... (1): Transparent9/3/0 (STANDBY - UP), Wave9/3 (UP)
                 : channel request: wait-to-restore
                 : switchover count: 1
                 : last switchover: 4 days, 25 minutes

```

Configuring the Search-For-Up Timer

The search-for-up timer on the Cisco ONS 15540 ESPx causes the system to wait for a splitter protection connection to come up before checking the other splitter protection connection.

When both members of a splitter pair are down, the system first checks one signal for the minimum time interval. If the splitter protection connection does not come up, the system checks the other connection and doubles the time interval. This process repeats until the maximum timer interval is reached or exceeded. Checking continues at the maximum timer interval until one of the splitter protection connections becomes active.

To configure the search-for-up timer, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# redundancy Switch(config-red)#	Enters redundancy configuration mode.
Step 2	Switch(config-red)# associate group name Switch(config-red-aps)#	Selects the interfaces to associate and enters APS configuration mode. Note The group name is case sensitive.
Step 3	Switch(config-red-aps)# aps disable	Disables the APS group.
Step 4	Switch(config-red-aps)# aps timer search-for-up min-interval max-interval	Modifies the timer that controls the check on the status of the working path. The default minimum interval is 2 seconds. The default maximum interval is 32 seconds.
Step 5	Switch(config-red-aps)# aps enable	Enables the APS group.

Example

The following example shows how to configure the search-for-up timer value for an APS group.

```

Switch(config)# redundancy
Switch(config-red)# associate group yc
Switch(config-red-aps)# aps disable
Switch(config-red-aps)# aps timer search-for-up 4 16
Switch(config-red-aps)# aps enable

```

Displaying the Search-For-Up Timer Configuration

To display the search-for-up timer configuration, use the following EXEC command:

Command	Purpose
show aps [detail group name interface { transparent <i>slot/subcard/0</i> wavepatch <i>slot/subcard/port</i> tengigethernetphy <i>slot/subcard</i> wdmsplit <i>slot/subcard/port</i> }]	Displays the APS configuration for interfaces and groups. Note Group names are case sensitive.

Example

The following example shows how to display the search-for-up configuration for an APS group:

```
Switch# show aps group splitter
```

```
APS Group splitter :
```

```
architecture.: 1+1, remote prov: unknown
span.....: end-to-end
prot. mode...: network side splitter
direction....: prov: uni, current: uni, remote prov: unknown
revertive....: no
aps state....: enabled (associated)
request timer: holddown: 5000 ms, max: 15000 ms, count 2
search-up-int: min: 4 secs, max: 16 secs
msg-channel..: auto (down)
created.....: 3 minutes
auto-failover: enabled
transmit k1k2: no-request, 0, 0, 1+1, uni
receive k1k2: no-request, 0, 0, unknown, unknown
switched chan: 0
protection(0): Wavepatch8/0/1 (STANDBY - UP)
                : channel request: no-request
                : switchover count: 0
                : last switchover: never
working... (1): Wavepatch8/0/0 (ACTIVE - UP)
                : channel request: no-request
                : switchover count: 0
                : last switchover: never
```

Configuring the Message Timers

The Cisco ONS 15540 ESPx provides two message timers, the APS message holddown timer and the APS message maximum inactivity interval timer. The APS message holddown timer prevents APS channel protocol message flooding. The maximum inactivity interval timer determines how often to send the inactivity messages to ensure that the APS channel protocol is still functioning between the nodes.

To configure the message timers, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# redundancy Switch(config-red)#	Enters redundancy configuration mode.
Step 2	Switch(config-red)# associate group <i>name</i> Switch(config-red-aps)#	Selects the interfaces to associate and enters APS configuration mode. Note The group name is case sensitive.
Step 3	Switch(config-red-aps)# aps disable	Disables the APS group.
Step 4	Switch(config-red-aps)# aps timer message holddown <i>milliseconds</i> [<i>count number</i>]	Modifies the message holddown timer. The default interval is 5000 milliseconds and the default message count is 2.
Step 5	Switch(config-red-aps)# aps timer message max-interval <i>seconds</i>	Modifies the message inactivity maximum interval timer. The default interval is 15 seconds.
Step 6	Switch(config-red-aps)# aps enable	Enables the APS group.

Example

The following example shows how to configure the message timer values for an APS group.

```
Switch(config)# redundancy
Switch(config-red)# associate group yc
Switch(config-red-aps)# aps disable
Switch(config-red-aps)# aps timer message holddown 4000 3
Switch(config-red-aps)# aps timer message max-interval 10
Switch(config-red-aps)# aps enable
```

Displaying the Message Timer Configuration

To display the message timer configuration, use the following EXEC command:

Command	Purpose
show aps [detail group <i>name</i> interface { transparent <i>slot/subcard/0</i> wavepatch <i>slot/subcard/port</i> tengigethernetphy <i>slot/subcard</i> wdmsplit <i>slot/subcard/port</i> }]	Displays the APS configuration for interfaces and groups. Note Group names are case sensitive.

Example

The following example shows how to display the message timer configuration for an APS group:

```
Switch# show aps group blue

APS Group blue :

architecture.: 1+1, remote prov: unknown
span.....: end-to-end
prot. mode...: network side splitter
direction...: prov: uni, current: uni, remote prov: unknown
revertive....: no
aps state....: enabled (associated)
→ request timer: holddown: 4000 ms, max: 10000 ms, count 3
search-up-int: min: 2 secs, max: 32 secs
msg-channel...: auto (down)
```

```

created.....: 3 minutes
auto-failover: enabled
transmit k1k2: no-request, 0, 0, 1+1, uni
receive k1k2: no-request, 0, 0, unknown, unknown
switched chan: 0
protection(0): Wavepatch8/0/1 (STANDBY - UP)
                : channel request: no-request
                : switchover count: 0
                : last switchover: never
working... (1): Wavepatch8/0/0 (ACTIVE - UP)
                : channel request: no-request
                : switchover count: 0
                : last switchover: never

```

Switchovers and Lockouts

In APS, you can switch a channel signal from one path to another, or you can lock out a switchover altogether while performing system maintenance.

A switchover of the channel signal from the working path to protection path is useful when upgrading or maintaining the system, or in cases where a signal failure caused a switchover. In the case of splitter protection, once the cause of the problem has been corrected, the system does not automatically revert to using the original working path. The switchover to the formerly failed interface must be requested from the CLI. The interface originally configured as the working path might be preferred because of its link loss characteristics or because of its distance advantage. For example, some protocols, such as ESCON, experience lower data throughput at increasing distances, so moving the signal back to the shorter path might be advised.

A lockout prevents a switchover of the active signal from the working path to the protection path. This is useful when upgrading or maintaining the system, or when the signal on the protection path has degraded or failed.

The Cisco ONS 15540 ESPx supports APS switchover and lockout requests from the CLI. These requests have priorities depending on the condition of the protection signal and the existence of other switchover requests. There are three types of switchover requests:

- Lockout requests—Have the highest priority and take effect regardless of the condition of the protection signal. A lockout prevents the active signal from switching over from the working path to the protection path.
- Forced switchover requests—Have the next highest priority and are only prevented if there is an existing lockout on the protection path, or the signal on the protection path has failed when switching from working to protection.
- Manual switchover requests—Have the lowest priority and only occur if there is no protection path lockout, a forced switchover, or the signal has failed or degraded.

In summary, the priority order is:

1. Lockout
2. Signal failure on the protection path
3. Forced switchover
4. Signal failure on the working path
5. Signal degrade on the working or protection path
6. Manual switchover

If a request or condition of a higher priority is in effect, a lower priority request is rejected.



Note

APS lockouts and switchovers do not persist across processor card switchovers or system reloads.

Requesting a Switchover or Lockout

To prevent switchovers to the protection signal, or to request a signal switchover, use the following commands in privileged EXEC mode:

Command	Purpose
<code>aps lockout group-name</code>	Locks out all switchovers to the protection path.
<code>aps switch group-name {force manual} {protection-to-working working-to-protection}</code>	Requests a signal switchover of the active signal from the working path to the protection path, or vice versa, within an associated interface pair.

Examples

The following example shows how to request a forced switchover from working to protection except if a lockout is in effect on the protection path:

```
Switch# aps switch blue force working-to-protection
```

The following example shows how to prevent a switchover to the protection path:

```
Switch# aps lockout Wavepatch3/0/0
```

Displaying Switchover and Lockout Request Status

To display a pending switchover request, use the following command in privileged EXEC mode:

Command	Purpose
<code>show aps [detail group name interface {transparent slot/subcard/0 wavepatch slot/subcard/port tengigethernetphy slot/subcard wdmsplit slot/subcard/port}]</code>	Displays the APS configuration for interfaces and groups. Note Group names are case sensitive.

The following example shows how to display the switchover request status on an APS group:

```
Switch# show aps group yellow
```

APS Group yellow:

```
architecture.: 1+1, remote prov: 1+1
span.....: end-to-end (client side y-cable)
direction....: prov: uni, current: uni, remote prov: bi
revertive....: no
created.....: 15 hours, 1 minute
aps state....: associated (enabled)
request timer: holddown: 5000 ms, max: 15000 ms, count 2
switched chan: 0
channel ( 0): Transparent4/3/0 (STANDBY - UP), Wave4/3 (UP)
→           : channel request: lockout-of-protection
```

```

→          : transmit request: lockout-of-protection
           : receive request: no-request
channel ( 1): Transparent2/3/0 (ACTIVE - UP), Wave2/3 (UP)
           : channel request: no-request
           : switchover count: 0
           : last switchover: never

```

Clearing Switchovers and Lockouts

A lockout or a forced or manual switchover request stays in effect until the system reboots. You can manually clear these requests from the CLI.

To clear an APS switchover or lockout, use the following privileged EXEC command:

Command	Purpose
<code>aps clear group-name</code>	Clears APS switch request or lockout on an associated interface pair.

Example

The following example shows how to clear the switchover requests on an associated interface pair using the default group name:

```
Switch# aps clear Wavepatch10/0/0
```

Displaying Switchover and Lockout Clear Status

To display a pending switchover request, use the following command in privileged EXEC mode:

Command	Purpose
<code>show aps [detail group name interface {transparent slot/subcard/0 wavepatch slot/subcard/port tengigethernetphy slot/subcard wdmsplit slot/subcard/port}]</code>	Displays the APS configuration for interfaces and groups. Note Group names are case sensitive.

The following example shows how to display the switchover requests status on an APS group:

```

Switch# show aps group blue

APS Group blue :

architecture.: 1+1, remote prov: 1+1
span.....: end-to-end (client side y-cable)
direction...: prov: uni, current: uni, remote prov: bi
revertive...: no
created.....: 15 hours, 1 minute
aps state...: associated (enabled)
request timer: holddown: 5000 ms, max: 15000 ms, count 2
switched chan: 0
→ channel ( 0): Transparent10/0/0 (STANDBY - UP)
→          : channel request: no-request
           : transmit request: no-request
           : receive request: no-request
channel ( 1): Transparent8/0/0 (ACTIVE - UP)

```

```
: channel request: no-request  
: switchover count: 0  
: last switchover: never
```




Configuring Dual Shelf Nodes

This chapter describes how to configure a dual shelf node in a network topology. This chapter contains the following sections:

- About Dual Shelf Nodes, page 8-1
- Configuring Line Card Protected Dual Shelf Nodes, page 8-1

About Dual Shelf Nodes

On a single Cisco ONS 15540 ESPx shelf, only 16 channels can be supported with line card protection. By cascading two Cisco ONS 15540 ESPx shelves, up to 32 channels can be supported with line card protection. You can use dual shelf nodes in either a point-to-point topology or a ring topology. The OSCs (optical supervisory channels) can both connect to one shelf, or they can be split between the two shelves.

Configuring Line Card Protected Dual Shelf Nodes

To configure a dual shelf node with line card protection, follow these steps:

-
- Step 1** Populate the shelves with the motherboards, modules, and processor cards.
 - Step 2** Connect the mux/demux modules with cables and configure the patch connections.
For more information on patch connections, see the “About Patch Connections” section on page 4-21.
 - Step 3** Establish network access to both shelves.
For information on configuring network access, see the “Configuring IP Access on the NME Interface” section on page 3-3.
 - Step 4** Configure IP addresses on the OSC wave interfaces.
For information on configuring an IP address on the OSC wave interface, see the “Configuring IP on the OSC” section on page 11-9.
 - Step 5** Configure the network topology information for the connections between the two shelves.
 - Step 6** Configure APS (Automatic Protection Switching) on the shelves in the network that support the channels.
-

Configuring and Cabling the Shelves

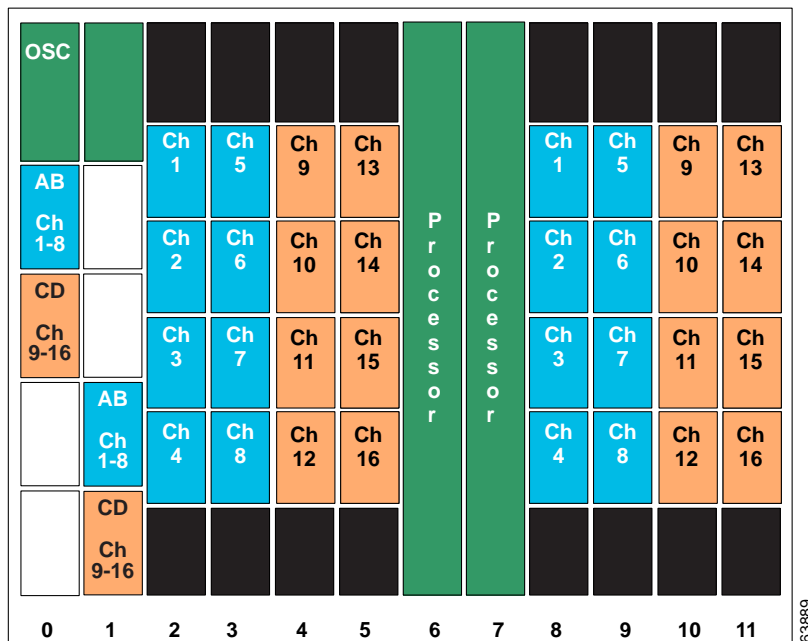
You can use add/drop mux/demux modules in a dual shelf node. For configurations with fewer than 32 channels in line card protection, use 8-channel add/drop mux/demux modules as often as possible.

Add/Drop Mux/Demux Modules for 24 Channels

Shelf 1 is configured for channels 1–16 with OSC to the west and shelf 2 is configured for channels 17–24 with OSC to the east. The mux/demux modules are patched between the two shelves as if they were in the same shelf.

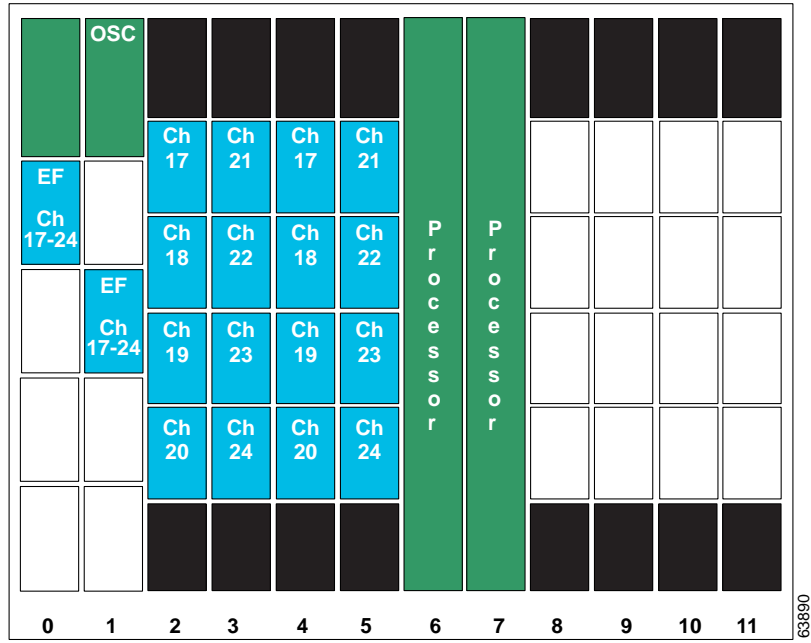
Figure 8-1 shows how the modules are installed for shelf 1 in the line card protected 24-channel configuration.

Figure 8-1 Shelf 1 Configuration for 24 Channels with Add/Drop Mux/Demux Modules and Line Card Protection



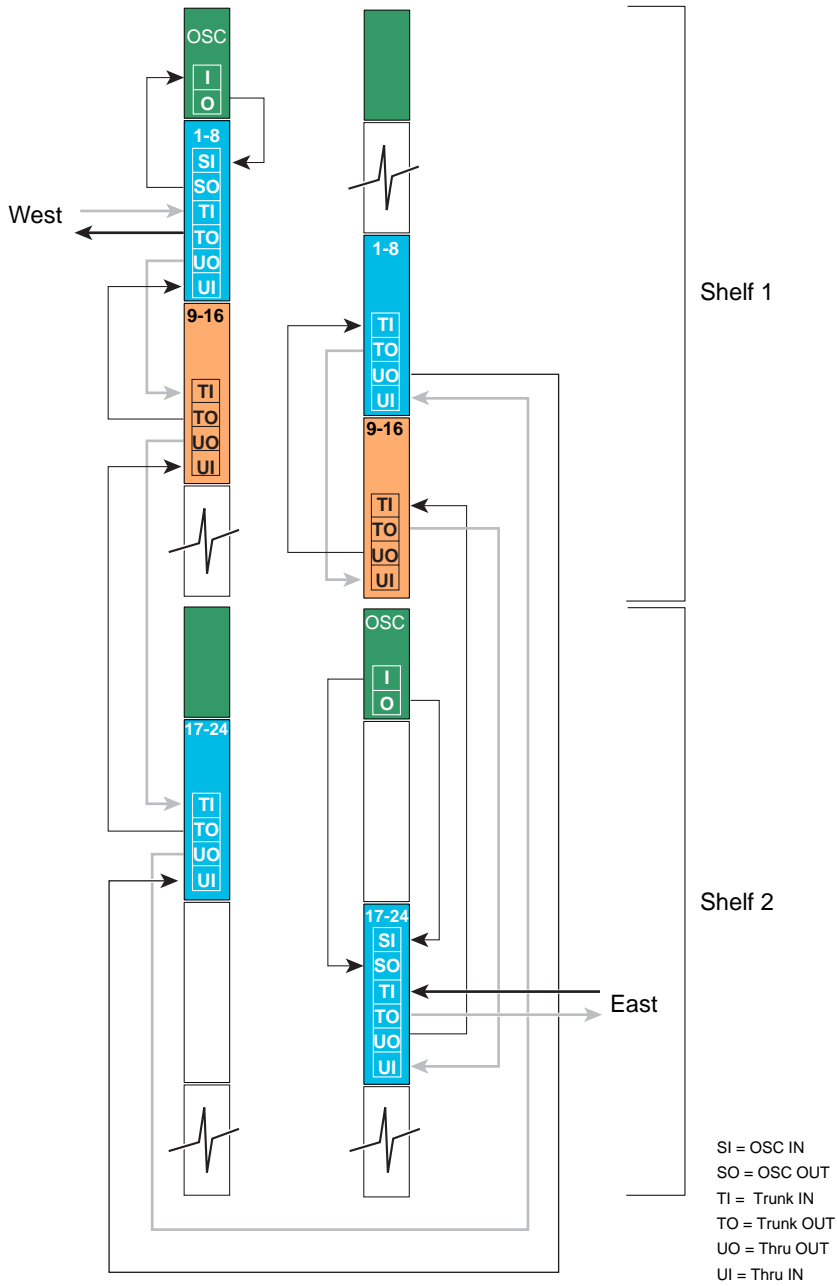
The configuration for shelf 2 is shown in Figure 8-2. As in shelf 1, unprotected line card motherboards are used in slots 2–5.

Figure 8-2 Shelf 2 Configuration for 24 Channels with Add/Drop Mux/Demux Modules and Line Card Protection



63890

Figure 8-3 Add/Drop Mux/Demux Module Cabling with Two Shelves with 24 Channels and Line Card Protection



63888

Configuring Connections Between Shelves

To include the two shelves as one node in the network topology, you must configure the patch connection between the shelves in the CLI (command-line interface). To configure these connections, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch1(config)# interface { <i>wave slot</i> oscfiler <i>slot/subcard</i> thru <i>slot/subcard</i> wdm <i>slot/subcard</i> }	Selects the interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# topology neighbor { <i>name node-name</i> ip-address <i>node-ip-address</i> mac-address <i>node-mac-address</i> } { port { <i>name port-name</i> ip-address <i>port-ip-address</i> mac-address <i>port-mac-address</i> } }	Configures the network topology information for a neighboring node.
Step 3	Switch(config-if)# topology neighbor agent ip-address <i>ip-address</i>	Specifies the address of the network topology agent on a neighboring node.



Note

Configure the patch connections between the mux/demux modules on the same shelf as described in the “About Patch Connections” section on page 4-21.

The following example shows how to configure the patch connections between the add/drop mux/demux modules on the two shelves in the node:

```
Shelf1(config)# interface thru 0/3
Shelf1(config-if)# topology neighbor name shelf2 port name wdm 0/0
Shelf1(config-if)# topology neighbor agent ip-address 10.2.2.4
Shelf1(config-if)# exit
Shelf1(config)# interface wdm 1/3
Shelf1(config-if)# topology neighbor name shelf2 port name thru 1/0
Shelf1(config-if)# topology neighbor agent ip-address 10.2.2.4
Shelf1(config-if)# exit

Shelf2(config)# interface wdm 0/0
Shelf2(config-if)# topology neighbor name shelf1 port name thru 0/3
Shelf2(config-if)# topology neighbor agent ip-address 10.2.2.4
Shelf2(config-if)# exit
Shelf2(config)# interface thru 1/0
Shelf2(config-if)# topology neighbor name shelf1 port name wdm 0/0
Shelf2(config-if)# topology neighbor agent ip-address 10.2.2.4
Shelf2(config-if)# exit
```

Configuring APS

When a dual shelf node is part of a network topology, the channels supported by it might require special configuration. On a dual shelf node, the OSC might have only one connection, such as the configuration shown in Figure 8-1 on page 8-2. For the APS Channel Protocol to function correctly, the shelves that support a channel must both have two OSC connections, or you must configure the APS group name and IP address information on the shelves.

To configure APS for a channel supported on a dual shelf node without full OSC support, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch1(config)# redundancy Switch1(config-red)#	Enters redundancy configuration mode.
Step 2	Switch(config-red)# associate group <i>name</i> Switch(config-red-aps)#	Specifies an APS group name and enters APS configuration mode. Note The group name is case sensitive.
Step 3	Switch(config-red-aps)# aps disable	Disables APS activity between the interfaces. Note For newly created APS groups, APS activity is disabled by default.
Step 4	Switch(config-red-aps)# aps working wavepatch <i>slot/subcard/port</i>	Configures the working path interface.
Step 5	Switch(config-red-aps)# aps protection wavepatch <i>slot/subcard/port</i>	Configures the protection path interface.
Step 6	Switch1(config-red-aps)# aps y-cable	Enables y-cable protection. The default state is no y-cable protection (disabled).
Step 7	Switch1(config-red-aps)# aps far-end group <i>group-name ip-address address</i>	Configures the APS group name and IP address on the remote node that support the channel.
Step 8	Switch1(config-red-aps)# aps enable	Enables APS activity between the interfaces.

For more information on configuring y-cable line card protection, refer to the “Configuring Y-Cable Based Line Card Protection” section on page 7-8.

Examples

For these examples, assume the following:

- Channels 17-20 terminate on the second shelf of the dual shelf node.
- The management IP address of the second shelf of the dual shelf node is 10.1.2.3.
- The management IP address of the single shelf node is 10.3.2.1.

The following example shows how to configure channels 17-20 on the single shelf node:

```
Switch(config)# redundancy
Switch(config-red)# associate group Channel17
Switch(config-red-aps)# aps working transparent 2/0/0
Switch(config-red-aps)# aps protection transparent 4/0/0
Switch(config-red-aps)# aps y-cable
Switch(config-red-aps)# aps far-end group Channel17 ip-address 10.1.2.3
Switch(config-red-aps)# aps enable
Switch(config-red-aps)# exit
Switch(config-red)# associate group Channel18
Switch(config-red-aps)# aps working transparent 2/1/0
Switch(config-red-aps)# aps protection transparent 4/1/0
Switch(config-red-aps)# aps y-cable
Switch(config-red-aps)# aps far-end group Channel18 ip-address 10.1.2.3
Switch(config-red-aps)# aps enable
Switch(config-red-aps)# exit
Switch(config-red)# associate group Channel19
Switch(config-red-aps)# aps working transparent 2/2/0
Switch(config-red-aps)# aps protection transparent 4/2/0
```

```

Switch(config-red-aps)# aps y-cable
Switch(config-red-aps)# aps far-end group Channel19 ip-address 10.1.2.3
Switch(config-red-aps)# aps enable
Switch(config-red-aps)# exit
Switch(config-red)# associate group Channel20
Switch(config-red-aps)# aps working transparent 2/3/0
Switch(config-red-aps)# aps protection transparent 4/3/0
Switch(config-red-aps)# aps y-cable
Switch(config-red-aps)# aps far-end group Channel20 ip-address 10.1.2.3
Switch(config-red-aps)# aps enable
Switch(config-red-aps)# end

Switch# copy system:running-config nvram:startup-config

```

The following example shows how to configure channels 17-20 on shelf 2 of a dual shelf node.

```

Shelf2(config)# redundancy
Shelf2(config-red)# associate group Channel17
Shelf2(config-red-aps)# aps working transparent 2/0/0
Shelf2(config-red-aps)# aps protection transparent 4/0/0
Shelf2(config-red-aps)# aps y-cable
Shelf2(config-red-aps)# aps far-end group Channel17 ip-address 10.3.2.1
Shelf2(config-red-aps)# aps enable
Shelf2(config-red-aps)# exit
Shelf2(config-red)# associate group Channel18
Shelf2(config-red-aps)# aps working transparent 2/1/0
Shelf2(config-red-aps)# aps protection transparent 4/1/0
Shelf2(config-red-aps)# aps y-cable
Shelf2(config-red-aps)# aps far-end group Channel18 ip-address 10.3.2.1
Shelf2(config-red-aps)# aps enable
Shelf2(config-red-aps)# exit
Shelf2(config-red)# associate group Channel19
Shelf2(config-red-aps)# aps working transparent 2/2/0
Shelf2(config-red-aps)# aps protection transparent 4/2/0
Shelf2(config-red-aps)# aps y-cable
Shelf2(config-red-aps)# aps far-end group Channel19 ip-address 10.3.2.1
Shelf2(config-red-aps)# aps enable
Shelf2(config-red-aps)# exit
Shelf2(config-red)# associate group Channel20
Shelf2(config-red-aps)# aps working transparent 2/3/0
Shelf2(config-red-aps)# aps protection transparent 4/3/0
Shelf2(config-red-aps)# aps y-cable
Shelf2(config-red-aps)# aps far-end group Channel20 ip-address 10.3.2.1
Shelf2(config-red-aps)# aps enable
Shelf2(config-red-aps)# end

Shelf2# copy system:running-config nvram:startup-config

```




Configuring Point-to-Point Topologies

This chapter describes how to configure point-to-point topologies. This chapter contains the following sections:

- About Point-to-Point Topologies, page 9-1
- Configuring a Point-to-Point Topology with Splitter Protection, page 9-3
- Configuring a Point-to-Point Topology with Line Card Protection, page 9-9
- Configuring an Unprotected Point-to-Point Topology, page 9-17

About Point-to-Point Topologies

In a point-to-point topology, two Cisco ONS 15540 ESPx systems are connected to each other in the network. Each of the systems originates and terminates all configured channels. You can use splitter protection to protect against fiber failure, or line card protection to protect against both the fiber and transponder failures. To also protect against client failure, you can implement protection on the client equipment itself.



Note

Client protection implementation is beyond the scope of this document.

Up to 32 client signals in splitter protection mode, or 16 client signals in line card protection mode, are optically multiplexed at each end and are multiplexed onto a single fiber pair. Figure 9-1 shows an example of this topology using two DWDM fiber links, one working and one protection.

Figure 9-1 Protected Point-to-Point Topology Example

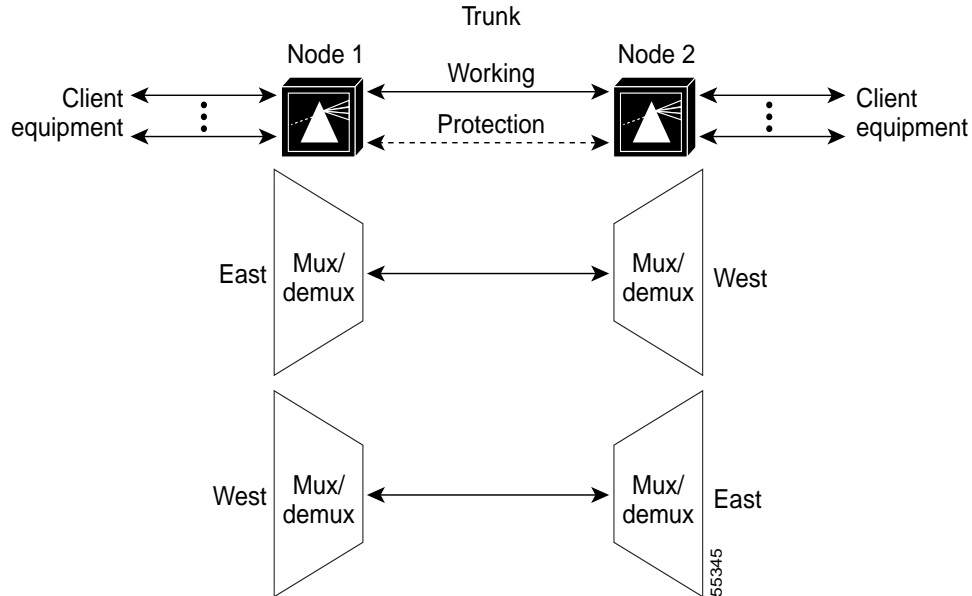
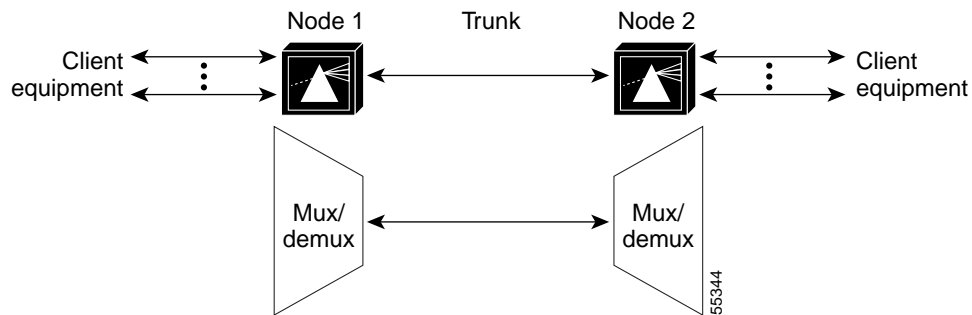


Figure 9-2 shows an example of an unprotected point-to-point topology using one unprotected DWDM fiber link.

Figure 9-2 Unprotected Point-to-Point Topology Example



Point-to-point topologies have many common applications, including extending the reach of Gigabit Ethernet or SONET in long-haul transport.

**Note**

Point-to-point topologies support an intermediate add/drop node only in an unprotected configuration. If add/drop with protection is required, a ring configuration should be used.

For more information on point-to-point topologies, refer to the *Cisco ONS 15540 ESPx Planning Guide*.

Multiple Trunk Support

You can connect two or more trunk fibers to you Cisco ONS 15540 ESPx and support multiple point-to-point topologies or a combination of point-to-point topologies and ring topologies. The configuration of the shelf is the same for all trunks except for the OSC support. If one of the topologies uses the OSC as the APS message channel, it is unavailable for management for the other topologies. In that case, you can use either the in-band message channel, if available, or an IP connection.

Configuring a Point-to-Point Topology with Splitter Protection

Figure 9-3 shows how the modules are installed in the shelf for a 32-channel point-to-point topology. Thirty-two client signals of any supported protocol are carried over the trunk fiber, which is protected. This scenario assumes that splitter protection is being used and the working path is through slot 0 on both nodes.

Figure 9-3 Shelf Configuration for Splitter Protected 32-Channel Point-to-Point Topology

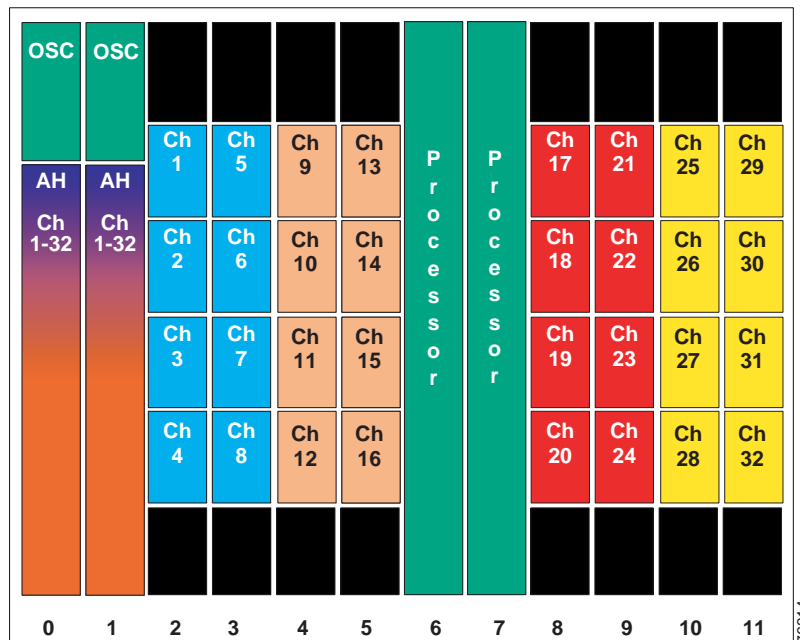
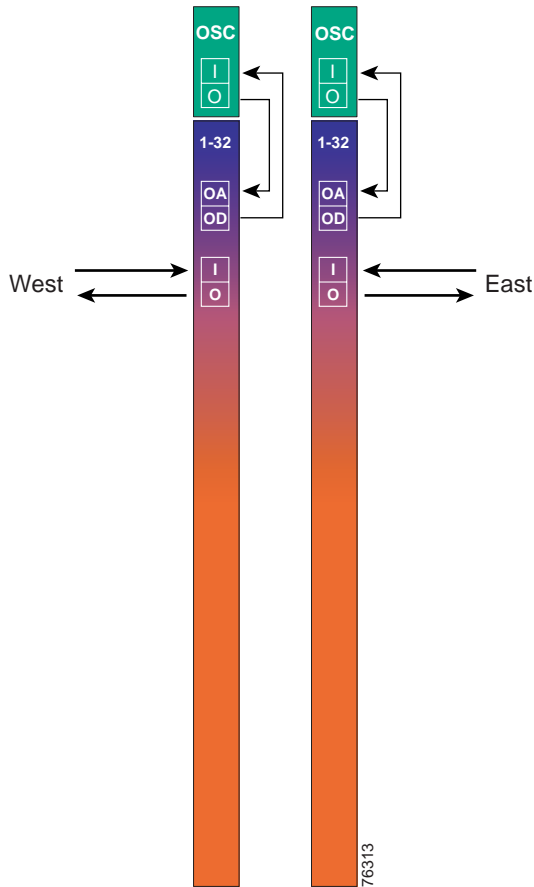


Figure 9-4 shows how the terminal mux/demux modules are cabled for the 32-channel splitter protected point-to-point configuration.

Figure 9-4 Terminal Mux/Demux Module Cabling with OSC for Splitter Protected 32-Channel Point-to-Point Topology



Patch Connections

```

Node1# configure terminal
Node1(config)# patch wave 0 oscfilter 0/0
Node1(config)# patch wave 1 oscfilter 1/0

Node1(config)# patch wavepatch 2/0/0 filter 0/0/0
Node1(config)# patch wavepatch 2/1/0 filter 0/0/1
Node1(config)# patch wavepatch 2/2/0 filter 0/0/2
Node1(config)# patch wavepatch 2/3/0 filter 0/0/3
Node1(config)# patch wavepatch 2/0/1 filter 1/0/0
Node1(config)# patch wavepatch 2/1/1 filter 1/0/1
Node1(config)# patch wavepatch 2/2/1 filter 1/0/2
Node1(config)# patch wavepatch 2/3/1 filter 1/0/3

Node1(config)# patch wavepatch 3/0/0 filter 0/0/4
Node1(config)# patch wavepatch 3/1/0 filter 0/0/5
Node1(config)# patch wavepatch 3/2/0 filter 0/0/6
Node1(config)# patch wavepatch 3/3/0 filter 0/0/7
Node1(config)# patch wavepatch 3/0/1 filter 1/0/4
Node1(config)# patch wavepatch 3/1/1 filter 1/0/5
Node1(config)# patch wavepatch 3/2/1 filter 1/0/6
Node1(config)# patch wavepatch 3/3/1 filter 1/0/7

```



```

Node1(config)# patch wavepatch 4/0/0 filter 0/0/8
Node1(config)# patch wavepatch 4/1/0 filter 0/0/9
Node1(config)# patch wavepatch 4/2/0 filter 0/0/10
Node1(config)# patch wavepatch 4/3/0 filter 0/0/11
Node1(config)# patch wavepatch 4/0/1 filter 1/0/8
Node1(config)# patch wavepatch 4/1/1 filter 1/0/9
Node1(config)# patch wavepatch 4/2/1 filter 1/0/10
Node1(config)# patch wavepatch 4/3/1 filter 1/0/11

Node1(config)# patch wavepatch 5/0/0 filter 0/0/12
Node1(config)# patch wavepatch 5/1/0 filter 0/0/13
Node1(config)# patch wavepatch 5/2/0 filter 0/0/14
Node1(config)# patch wavepatch 5/3/0 filter 0/0/15
Node1(config)# patch wavepatch 5/0/1 filter 1/0/12
Node1(config)# patch wavepatch 5/1/1 filter 1/0/13
Node1(config)# patch wavepatch 5/2/1 filter 1/0/14
Node1(config)# patch wavepatch 5/3/1 filter 1/0/15

Node1(config)# patch wavepatch 8/0/0 filter 0/0/16
Node1(config)# patch wavepatch 8/1/0 filter 0/0/17
Node1(config)# patch wavepatch 8/2/0 filter 0/0/18
Node1(config)# patch wavepatch 8/3/0 filter 0/0/19
Node1(config)# patch wavepatch 8/0/1 filter 1/0/16
Node1(config)# patch wavepatch 8/1/1 filter 1/0/17
Node1(config)# patch wavepatch 8/2/1 filter 1/0/18
Node1(config)# patch wavepatch 8/3/1 filter 1/0/19

Node1(config)# patch wavepatch 9/0/0 filter 0/0/20
Node1(config)# patch wavepatch 9/1/0 filter 0/0/20
Node1(config)# patch wavepatch 9/2/0 filter 0/0/22
Node1(config)# patch wavepatch 9/3/0 filter 0/0/23
Node1(config)# patch wavepatch 9/0/1 filter 1/0/20
Node1(config)# patch wavepatch 9/1/1 filter 1/0/20
Node1(config)# patch wavepatch 9/2/1 filter 1/0/22
Node1(config)# patch wavepatch 9/3/1 filter 1/0/23

Node1(config)# patch wavepatch 10/0/0 filter 0/0/24
Node1(config)# patch wavepatch 10/1/0 filter 0/0/25
Node1(config)# patch wavepatch 10/2/0 filter 0/0/26
Node1(config)# patch wavepatch 10/3/0 filter 0/0/27
Node1(config)# patch wavepatch 10/0/1 filter 1/0/24
Node1(config)# patch wavepatch 10/1/1 filter 1/0/25
Node1(config)# patch wavepatch 10/2/1 filter 1/0/26
Node1(config)# patch wavepatch 10/3/1 filter 1/0/27

Node1(config)# patch wavepatch 11/0/0 filter 0/0/28
Node1(config)# patch wavepatch 11/1/0 filter 0/0/29
Node1(config)# patch wavepatch 11/2/0 filter 0/0/30
Node1(config)# patch wavepatch 11/3/0 filter 0/0/31
Node1(config)# patch wavepatch 11/0/1 filter 1/0/28
Node1(config)# patch wavepatch 11/1/1 filter 1/0/29
Node1(config)# patch wavepatch 11/2/1 filter 1/0/30
Node1(config)# patch wavepatch 11/3/1 filter 1/0/31

```

Transparent Interfaces

```

Node1(config)# interface transparent 2/0/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit

```

```
Node1(config)# interface transparent 2/1/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 2/1
Node1(config-if)# laser frequency 192200
Node1(config-if)# exit
```

```
Node1(config)# interface transparent 2/2/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
```

```
Node1(config)# interface transparent 2/3/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 2/3
Node1(config-if)# laser frequency 192400
Node1(config-if)# exit
```

```
Node1(config)# interface transparent 3/0/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
```

```
Node1(config)# interface transparent 3/1/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 3/1
Node1(config-if)# laser frequency 192700
Node1(config-if)# exit
```

```
Node1(config)# interface transparent 3/2/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
```

```
Node1(config)# interface transparent 3/3/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 3/3
Node1(config-if)# laser frequency 192900
Node1(config-if)# exit
```

```
Node1(config)# interface transparent 4/0/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
```

```
Node1(config)# interface transparent 4/1/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 4/1
Node1(config-if)# laser frequency 193200
Node1(config-if)# exit
```

```
Node1(config)# interface transparent 4/2/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
```

```
Node1(config)# interface transparent 4/3/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 4/3
Node1(config-if)# laser frequency 193400
Node1(config-if)# exit

Node1(config)# interface transparent 5/0/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 5/1/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 5/1
Node1(config-if)# laser frequency 193700
Node1(config-if)# exit

Node1(config)# interface transparent 5/2/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 5/3/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 5/3
Node1(config-if)# laser frequency 193900
Node1(config-if)# exit

Node1(config)# interface transparent 8/0/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 8/1/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 8/1
Node1(config-if)# laser frequency 194200
Node1(config-if)# exit

Node1(config)# interface transparent 8/2/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 8/3/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 8/3
Node1(config-if)# laser frequency 194400
Node1(config-if)# exit

Node1(config)# interface transparent 9/0/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
```

```
Node1(config-if)# exit

Node1(config)# interface transparent 9/1/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 9/1
Node1(config-if)# laser frequency 194700
Node1(config-if)# exit

Node1(config)# interface transparent 9/2/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 9/3/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 9/3
Node1(config-if)# laser frequency 194900
Node1(config-if)# exit

Node1(config)# interface transparent 10/0/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 10/1/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 10/1
Node1(config-if)# laser frequency 195200
Node1(config-if)# exit

Node1(config)# interface transparent 10/2/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 10/3/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 10/3
Node1(config-if)# laser frequency 195400
Node1(config-if)# exit

Node1(config)# interface transparent 11/0/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 11/1/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 11/1
Node1(config-if)# laser frequency 195700
Node1(config-if)# exit

Node1(config)# interface transparent 11/2/0
Node1(config-if)# encapsulation sonet oc12
```

```
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 11/3/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 11/3
Node1(config-if)# laser frequency 195900
Node1(config-if)# exit
```

APS

```
Node1(config)# redundancy
Node1(config-red)# associate interface wavepatch */*/0 wavepatch */*/1 enable
Node1(config-red)# end
```

```
Node1# copy system:running-config nvram:startup-config
```

Repeat the entire preceding configuration on node 2.

Configuring a Point-to-Point Topology with Line Card Protection

Figure 9-5 shows how the modules are installed in the shelf for a 16-channel point-to-point topology with line card protection. Sixteen client signals of any supported protocol are carried over the trunk fiber, which is also protected.



Note

For information about configuring nodes with more than 16 channels and line card protection, see Chapter 8, “Configuring Dual Shelf Nodes.”

Figure 9-5 Shelf Configuration for Line Card Protected 16-Channel Point-to-Point Topology

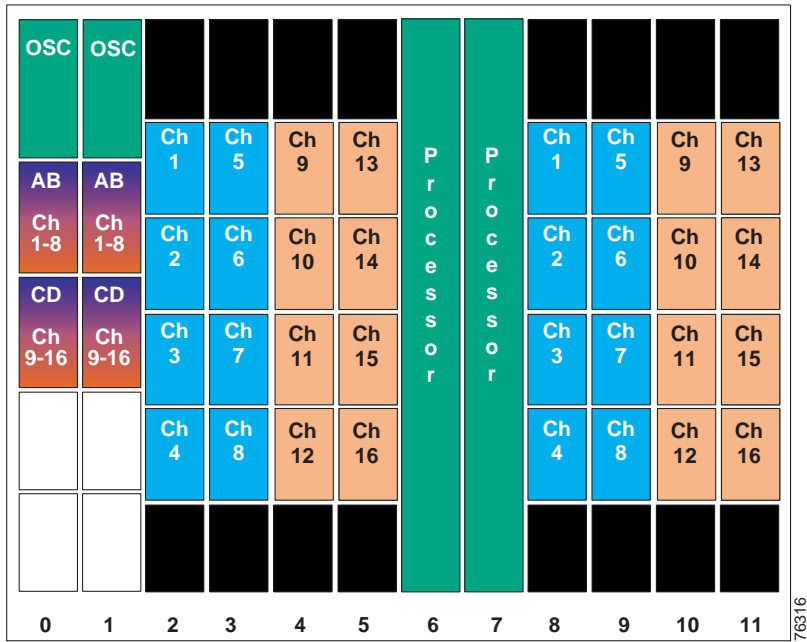
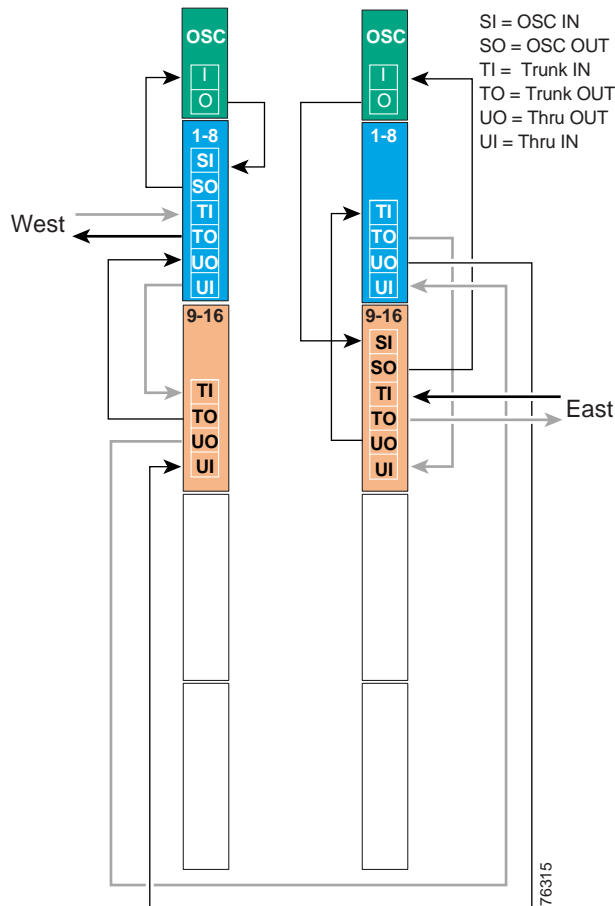


Figure 9-6 shows how the terminal mux/demux modules are cabled for the 16-channel line card protected point-to-point configuration.

Figure 9-6 Terminal Mux/Demux Module Cabling with OSC for Line Card Protected 16-Channel Point-to-Point Topology



Node 1

Patch Connections

```

Node1# configure terminal
Node1(config)# patch wave 0 oscfilter 0/0
Node1(config)# patch wave 1 oscfilter 1/1

Node1(config)# patch thru 0/0 wdm 0/1
Node1(config)# patch thru 0/1 thru 1/0
Node1(config)# patch wdm 1/0 thru 1/1

Node1(config)# patch wavepatch 2/0/0 filter 0/0/0
Node1(config)# patch wavepatch 2/1/0 filter 0/0/1
Node1(config)# patch wavepatch 2/2/0 filter 0/0/2
Node1(config)# patch wavepatch 2/3/0 filter 0/0/3

Node1(config)# patch wavepatch 3/0/0 filter 0/0/4
Node1(config)# patch wavepatch 3/1/0 filter 0/0/5
Node1(config)# patch wavepatch 3/2/0 filter 0/0/6
Node1(config)# patch wavepatch 3/3/0 filter 0/0/7
  
```

```

Node1(config)# patch wavepatch 4/0/0 filter 0/1/8
Node1(config)# patch wavepatch 4/1/0 filter 0/1/9
Node1(config)# patch wavepatch 4/2/0 filter 0/1/10
Node1(config)# patch wavepatch 4/3/0 filter 0/1/11

Node1(config)# patch wavepatch 5/0/0 filter 0/1/12
Node1(config)# patch wavepatch 5/1/0 filter 0/1/13
Node1(config)# patch wavepatch 5/2/0 filter 0/1/14
Node1(config)# patch wavepatch 5/3/0 filter 0/1/15

Node1(config)# patch wavepatch 8/0/0 filter 1/0/0
Node1(config)# patch wavepatch 8/1/0 filter 1/0/1
Node1(config)# patch wavepatch 8/2/0 filter 1/0/2
Node1(config)# patch wavepatch 8/3/0 filter 1/0/3

Node1(config)# patch wavepatch 9/0/0 filter 1/0/4
Node1(config)# patch wavepatch 9/1/0 filter 1/0/5
Node1(config)# patch wavepatch 9/2/0 filter 1/0/6
Node1(config)# patch wavepatch 9/3/0 filter 1/0/7

Node1(config)# patch wavepatch 10/0/0 filter 1/1/8
Node1(config)# patch wavepatch 10/1/0 filter 1/1/9
Node1(config)# patch wavepatch 10/2/0 filter 1/1/10
Node1(config)# patch wavepatch 10/3/0 filter 1/1/11

Node1(config)# patch wavepatch 11/0/0 filter 1/1/12
Node1(config)# patch wavepatch 11/1/0 filter 1/1/13
Node1(config)# patch wavepatch 11/2/0 filter 1/1/14
Node1(config)# patch wavepatch 11/3/0 filter 1/1/15

```

Transparent Interfaces

```

Node1(config)# interface transparent 2/0/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 2/1/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 2/1
Node1(config-if)# laser frequency 192200
Node1(config-if)# exit

Node1(config)# interface transparent 2/2/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 2/3/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 2/3
Node1(config-if)# laser frequency 192400
Node1(config-if)# exit

Node1(config)# interface transparent 3/0/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable

```



```
Node1(config-if)# exit

Node1(config)# interface transparent 3/1/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 3/1
Node1(config-if)# laser frequency 192700
Node1(config-if)# exit

Node1(config)# interface transparent 3/2/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 3/3/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 3/3
Node1(config-if)# laser frequency 192900
Node1(config-if)# exit

Node1(config)# interface transparent 4/0/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 4/1/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 4/1
Node1(config-if)# laser frequency 193200
Node1(config-if)# exit

Node1(config)# interface transparent 4/2/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 4/3/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 4/3
Node1(config-if)# laser frequency 193400
Node1(config-if)# exit

Node1(config)# interface transparent 5/0/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 5/1/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 5/1
Node1(config-if)# laser frequency 193700
Node1(config-if)# exit

Node1(config)# interface transparent 5/2/0
Node1(config-if)# encapsulation sonet oc12
```

```
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 5/3/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 5/3
Node1(config-if)# laser frequency 193900
Node1(config-if)# exit

Node1(config)# interface transparent 8/0/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 8/1/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 8/1
Node1(config-if)# laser frequency 192200
Node1(config-if)# exit

Node1(config)# interface transparent 8/2/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 8/3/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 8/3
Node1(config-if)# laser frequency 192400
Node1(config-if)# exit

Node1(config)# interface transparent 9/0/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 9/1/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 9/1
Node1(config-if)# laser frequency 192700
Node1(config-if)# exit

Node1(config)# interface transparent 9/2/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 9/3/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 9/3
Node1(config-if)# laser frequency 192900
Node1(config-if)# exit

Node1(config)# interface transparent 10/0/0
```

```

Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 10/1/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 10/1
Node1(config-if)# laser frequency 193200
Node1(config-if)# exit

Node1(config)# interface transparent 10/2/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 10/3/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 10/3
Node1(config-if)# laser frequency 193400
Node1(config-if)# exit

Node1(config)# interface transparent 11/0/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 11/1/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 11/1
Node1(config-if)# laser frequency 1953700
Node1(config-if)# exit

Node1(config)# interface transparent 11/2/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 11/3/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 11/3
Node1(config-if)# laser frequency 193900
Node1(config-if)# exit

```

APS

Use the following commands to configure y-cable protection. The working path is through slot 0.

```

Node1(config)# redundancy
Node1(config-red)# associate group channel1
Node1(config-red-aps)# aps working transparent 2/0/0
Node1(config-red-aps)# aps protection transparent 8/0/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel2

```

```

Node1(config-red-aps)# aps working transparent 2/1/0
Node1(config-red-aps)# aps protection transparent 8/1/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel3
Node1(config-red-aps)# aps working transparent 2/2/0
Node1(config-red-aps)# aps protection transparent 8/2/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel4
Node1(config-red-aps)# aps working transparent 2/3/0
Node1(config-red-aps)# aps protection transparent 8/3/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel5
Node1(config-red-aps)# aps working transparent 3/0/0
Node1(config-red-aps)# aps protection transparent 9/0/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel6
Node1(config-red-aps)# aps working transparent 3/1/0
Node1(config-red-aps)# aps protection transparent 9/1/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel7
Node1(config-red-aps)# aps working transparent 3/2/0
Node1(config-red-aps)# aps protection transparent 9/2/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel8
Node1(config-red-aps)# aps working transparent 3/3/0
Node1(config-red-aps)# aps protection transparent 9/3/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel9
Node1(config-red-aps)# aps working transparent 4/0/0
Node1(config-red-aps)# aps protection transparent 10/0/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel10
Node1(config-red-aps)# aps working transparent 4/1/0
Node1(config-red-aps)# aps protection transparent 10/1/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel11
Node1(config-red-aps)# aps working transparent 4/2/0
Node1(config-red-aps)# aps protection transparent 10/2/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel12
Node1(config-red-aps)# aps working transparent 4/3/0
Node1(config-red-aps)# aps protection transparent 10/3/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps enable

```

```
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel13
Node1(config-red-aps)# aps working transparent 5/0/0
Node1(config-red-aps)# aps protection transparent 11/0/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel14
Node1(config-red-aps)# aps working transparent 5/1/0
Node1(config-red-aps)# aps protection transparent 11/0/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel15
Node1(config-red-aps)# aps working transparent 5/2/0
Node1(config-red-aps)# aps protection transparent 11/2/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel16
Node1(config-red-aps)# aps working transparent 5/3/0
Node1(config-red-aps)# aps protection transparent 11/3/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# end

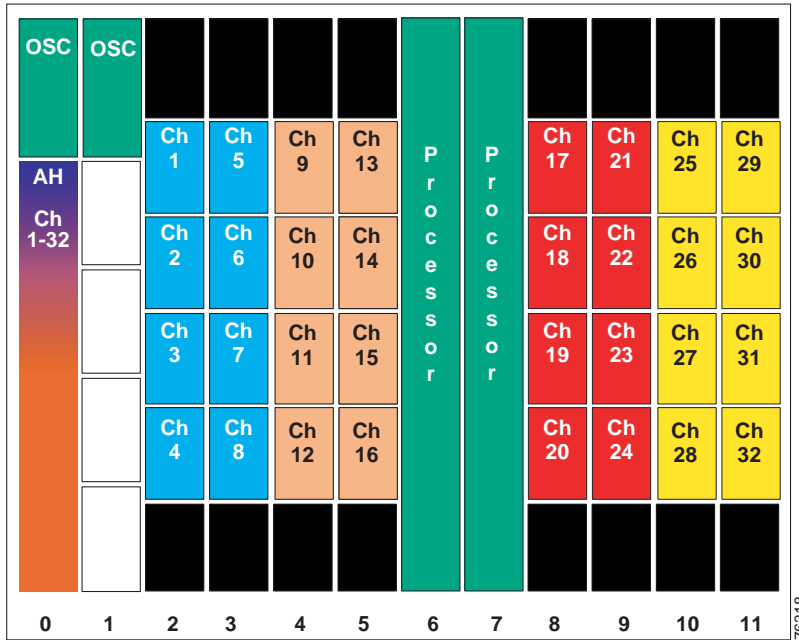
Node1# copy system:running-config nvram:startup-config
```

Repeat the entire preceding configuration on node 2.

Configuring an Unprotected Point-to-Point Topology

Figure 9-7 shows how the modules are installed in the shelf for a 32-channel point-to-point topology without protection.

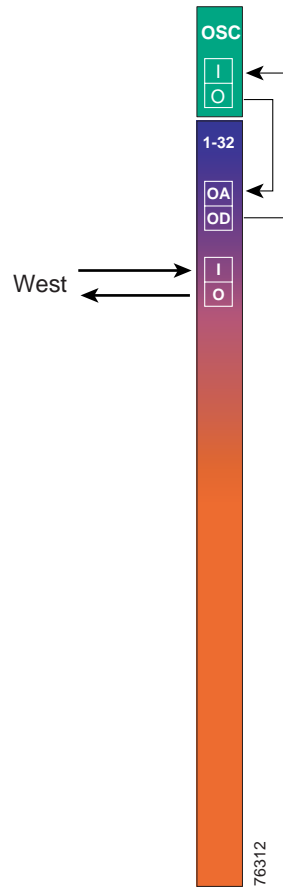
Figure 9-7 Shelf Configuration for Unprotected 32-Channel Point-to-Point Topology



76318

Figure 9-8 shows how the terminal mux/demux modules are cabled for the 32-channel unprotected point-to-point configuration.

Figure 9-8 Terminal Mux/Demux Module Cabling with OSC for Unprotected 32-Channel Point-to-Point Topology



Patch Connections

Node 1

```

Node1# configure terminal
Node1(config)# patch wave 0 oscfilter 0/0

Node1(config)# patch wavepatch 2/0/0 filter 0/0/0
Node1(config)# patch wavepatch 2/1/0 filter 0/0/1
Node1(config)# patch wavepatch 2/2/0 filter 0/0/2
Node1(config)# patch wavepatch 2/3/0 filter 0/0/3

Node1(config)# patch wavepatch 3/0/0 filter 0/0/4
Node1(config)# patch wavepatch 3/1/0 filter 0/0/5
Node1(config)# patch wavepatch 3/2/0 filter 0/0/6
Node1(config)# patch wavepatch 3/3/0 filter 0/0/7

Node1(config)# patch wavepatch 4/0/0 filter 0/0/8
Node1(config)# patch wavepatch 4/1/0 filter 0/0/9
Node1(config)# patch wavepatch 4/2/0 filter 0/0/10
Node1(config)# patch wavepatch 4/3/0 filter 0/0/11

Node1(config)# patch wavepatch 5/0/0 filter 0/0/12

```

```

Node1 (config)# patch wavepatch 5/1/0 filter 0/0/13
Node1 (config)# patch wavepatch 5/2/0 filter 0/0/14
Node1 (config)# patch wavepatch 5/3/0 filter 0/0/15

Node1 (config)# patch wavepatch 8/0/0 filter 0/0/16
Node1 (config)# patch wavepatch 8/1/0 filter 0/0/17
Node1 (config)# patch wavepatch 8/2/0 filter 0/0/18
Node1 (config)# patch wavepatch 8/3/0 filter 0/0/19

Node1 (config)# patch wavepatch 9/0/0 filter 0/0/20
Node1 (config)# patch wavepatch 9/1/0 filter 0/0/20
Node1 (config)# patch wavepatch 9/2/0 filter 0/0/22
Node1 (config)# patch wavepatch 9/3/0 filter 0/0/23

Node1 (config)# patch wavepatch 10/0/0 filter 0/0/24
Node1 (config)# patch wavepatch 10/1/0 filter 0/0/25
Node1 (config)# patch wavepatch 10/2/0 filter 0/0/26
Node1 (config)# patch wavepatch 10/3/0 filter 0/0/27

Node1 (config)# patch wavepatch 11/0/0 filter 0/0/28
Node1 (config)# patch wavepatch 11/1/0 filter 0/0/29
Node1 (config)# patch wavepatch 11/2/0 filter 0/0/30
Node1 (config)# patch wavepatch 11/3/0 filter 0/0/31

```

Node 2

```

Node2# configure terminal
Node2 (config)# patch wave 0 oscfilter 0/0

Node1 (config)# patch wavepatch 2/0/0 filter 0/0/0
Node1 (config)# patch wavepatch 2/1/0 filter 0/0/1
Node1 (config)# patch wavepatch 2/2/0 filter 0/0/2
Node1 (config)# patch wavepatch 2/3/0 filter 0/0/3

Node1 (config)# patch wavepatch 3/0/0 filter 0/0/4
Node1 (config)# patch wavepatch 3/1/0 filter 0/0/5
Node1 (config)# patch wavepatch 3/2/0 filter 0/0/6
Node1 (config)# patch wavepatch 3/3/0 filter 0/0/7

Node1 (config)# patch wavepatch 4/0/0 filter 0/0/8
Node1 (config)# patch wavepatch 4/1/0 filter 0/0/9
Node1 (config)# patch wavepatch 4/2/0 filter 0/0/10
Node1 (config)# patch wavepatch 4/3/0 filter 0/0/11

Node1 (config)# patch wavepatch 5/0/0 filter 0/0/12
Node1 (config)# patch wavepatch 5/1/0 filter 0/0/13
Node1 (config)# patch wavepatch 5/2/0 filter 0/0/14
Node1 (config)# patch wavepatch 5/3/0 filter 0/0/15

Node1 (config)# patch wavepatch 8/0/0 filter 0/0/16
Node1 (config)# patch wavepatch 8/1/0 filter 0/0/17
Node1 (config)# patch wavepatch 8/2/0 filter 0/0/18
Node1 (config)# patch wavepatch 8/3/0 filter 0/0/19

Node1 (config)# patch wavepatch 9/0/0 filter 0/0/20
Node1 (config)# patch wavepatch 9/1/0 filter 0/0/20
Node1 (config)# patch wavepatch 9/2/0 filter 0/0/22
Node1 (config)# patch wavepatch 9/3/0 filter 0/0/23

Node1 (config)# patch wavepatch 10/0/0 filter 0/0/24
Node1 (config)# patch wavepatch 10/1/0 filter 0/0/25
Node1 (config)# patch wavepatch 10/2/0 filter 0/0/26
Node1 (config)# patch wavepatch 10/3/0 filter 0/0/27

```



```
Node1(config)# patch wavepatch 11/0/0 filter 0/0/28
Node1(config)# patch wavepatch 11/1/0 filter 0/0/29
Node1(config)# patch wavepatch 11/2/0 filter 0/0/30
Node1(config)# patch wavepatch 11/3/0 filter 0/0/31
```

Transparent Interfaces

Node 1

```
Node1(config)# interface transparent 2/0/0
Node1(config-if)# encapsulation sonet oc12
Node1(config-if)# monitor enable
Node1(config-if)# exit
```

Configure the remaining transparent interfaces in the shelf the same as node 1 in the “Configuring a Point-to-Point Topology with Splitter Protection” section on page 9-3.

```
Node1# copy system:running-config nvram:startup-config
```

Node 2

```
Node2(config)# interface transparent 2/0/0
Node2(config-if)# encapsulation sonet oc12
Node2(config-if)# monitor enable
Node2(config-if)# end
```

Configure the remaining transparent interfaces in the shelf the same as node 1 in the “Configuring a Point-to-Point Topology with Splitter Protection” section on page 9-3.

```
Node2# copy system:running-config nvram:startup-config
```




Configuring Ring Topologies

This chapter describes how to configure the Cisco ONS 15540 ESPx in two-fiber topologies and provides example configurations for hubbed ring and meshed ring topologies using optical add/drop multiplexing. This chapter includes the following sections:

- About Ring Topologies, page 10-1
- Configuring a Hubbed Ring with Splitter Protection and OSC, page 10-3
- Configuring a Hubbed Ring with Line Card Protection and OSC, page 10-22
- Configuring a Meshed Ring with Splitter Protection and OSC, page 10-46
- Configuring a Splitter Protected Meshed Ring with Unprotected Channels and OSC, page 10-63
- Configuring a Meshed Ring with Line Card Protection and OSC, page 10-72
- Configuring a Line Card Protected Meshed Ring with Unprotected Channels and OSC, page 10-94

About Ring Topologies

A ring topology is a network of three or more nodes each of which connects to two other nodes to form a “ring”. Ring topologies support splitter protected, line card protected, and unprotected configurations. On a ring, traffic is transmitted in both directions from each node; traffic is received from only one direction. In case of a fiber failure, the node switches over to receive traffic from the other direction.

The Cisco ONS 15540 ESPx supports hubbed ring and meshed ring topologies.



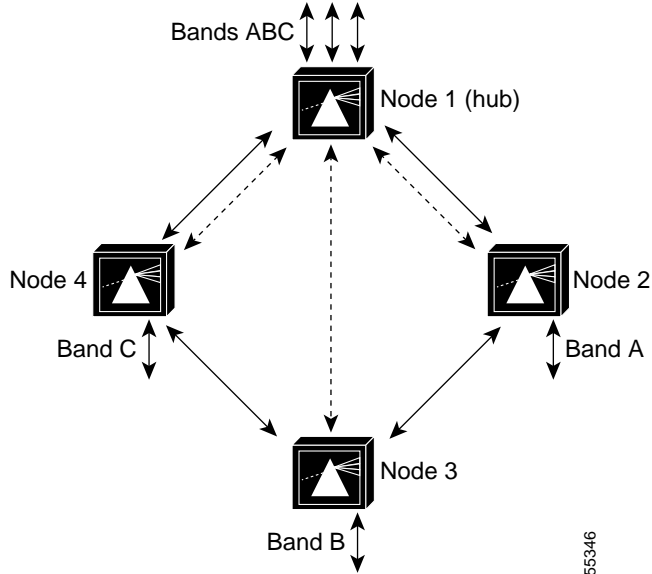
Note

We recommend ESCON for point-to-point topologies, not ring topologies.

Hubbed Ring Topologies

In a hubbed ring topology, all channels originate and terminate on the hub node (node1 in Figure 10-1). The other nodes on the ring, sometimes called *satellite nodes*, add and drop one or more channels. The added and dropped channels terminate at the node, while the channels that are not being dropped (express channels) are passed through optically, without being electrically terminated.

Figure 10-1 Hubbed Ring Topology Example



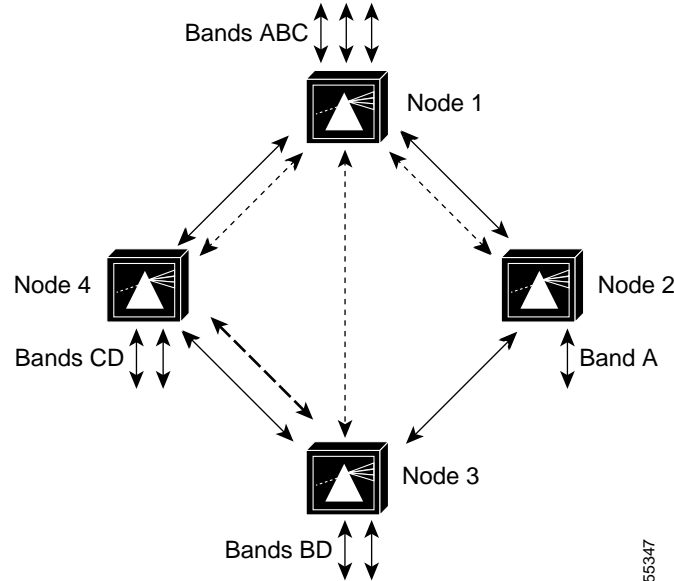
For more information on hubbed ring topologies, refer to the *Introduction to DWDM Technology* document and the *Cisco ONS 15540 ESPx Planning Guide*.

Meshed Ring Topologies

A meshed ring is a physical ring that has the characteristics of a mesh. Figure 10-2 shows an example of this type of configuration, which is sometimes called a *logical mesh*. While all traffic travels around the physical ring, nodes 1 and node 3 share band B (channels 5-8), and nodes 3 and node 4 share band D (channels 29-32). Hence there is a logical mesh overlay on the ring.

Protection options and optical link loss budget considerations are the same as in a hubbed ring configuration.

Figure 10-2 Meshed Ring Topology Example



For more information on meshed ring topologies, refer to the *Introduction to DWDM Technology* document and the *Cisco ONS 15540 ESPx Planning and Design Guide*.

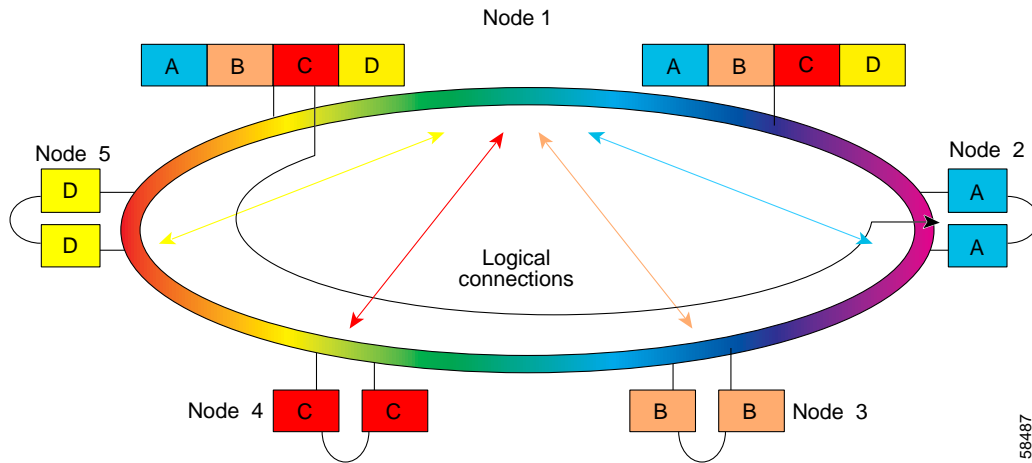
Multiple Trunk Support

You can connect two or more trunk fibers to you Cisco ONS 15540 ESPx and support multiple ring topologies or a combination of point-to-point topologies and ring topologies. The configuration of the shelf is the same for all trunks except for the OSC support. If one of the topologies uses the OSC as the APS message channel, it is unavailable for management for the other topologies. In that case, you can use either the in-band message channel, if available, or an IP connection.

Configuring a Hubbed Ring with Splitter Protection and OSC

Figure 10-3 shows an example topology of a three-node hubbed ring. Node 1 is the hub configured with band A through band D (channels 1-16). Node 2 adds and drops band A (channels 1-4), node 3 adds and drops band B (channels 5-8), node 4 adds and drops band C (channels 9-12), and node 5 adds and drops band D (channels 13-16). The transponders carry Gigabit Ethernet traffic.

Figure 10-3 Hubbed Ring Channel Plan



Node 1

Figure 10-4 shows how the modules are installed in the shelf for node 1 in the example network shown in Figure 10-3 on page 10-4. The shelf is populated for the 16-channel splitter protected hub node. Splitter line card motherboards are installed in slots 2–5, and the 16-channel terminal mux/demux modules are used in the west and east mux/demux slots 0 and 1. Each line card motherboard cross connects the signal to both mux/demux modules.

Figure 10-4 Shelf Configuration for 16-Channel Hub Node in Splitter Protected Hubbed Ring

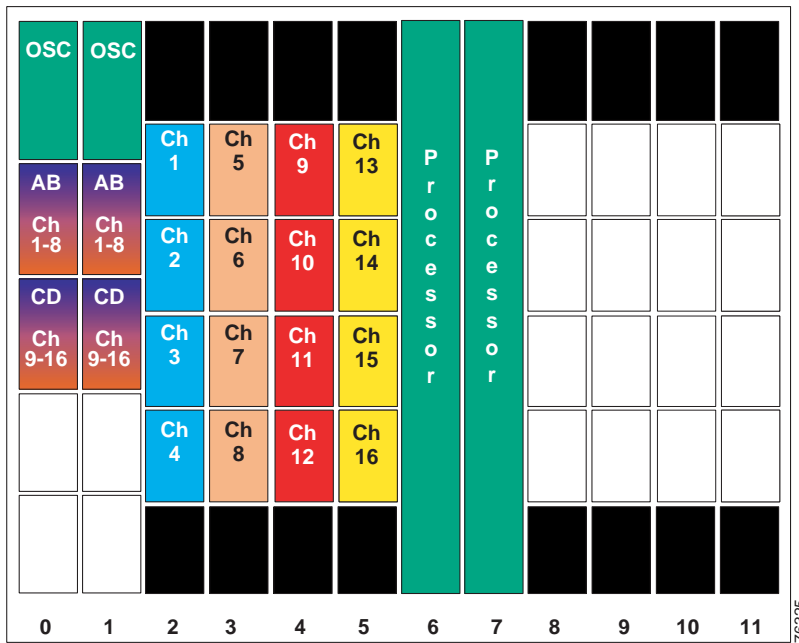
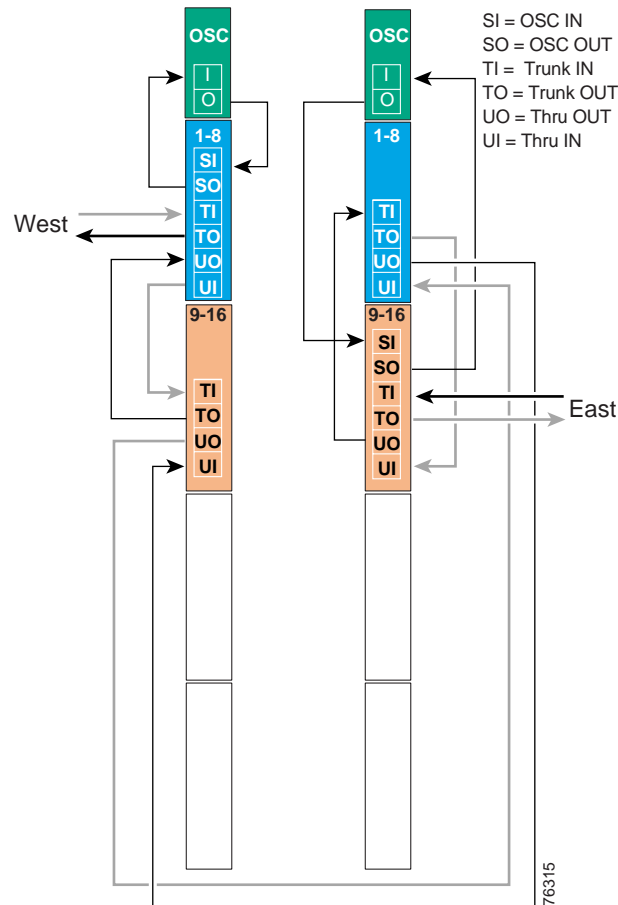


Figure 10-5 shows how the 8-channel mux/demux modules are cabled for the hub node in the splitter protected hubbed ring shown in Figure 10-3 on page 10-4.

Figure 10-5 Terminal Mux/Demux Module Cabling with OSC for 16-Channel Hub Node in Splitter Protected Hubbed Ring



Patch Connections

```

Node1# configure terminal
Node1(config)# patch wave 0 oscfilter 0/0
Node1(config)# patch wave 1 oscfilter 1/1

Node1(config)# patch thru 0/0 wdm 0/1
Node1(config)# patch thru 0/1 thru 1/0
Node1(config)# patch wdm 1/0 thru 1/1

Node1(config)# patch wavepatch 2/0/0 filter 0/0/0
Node1(config)# patch wavepatch 2/1/0 filter 0/0/1
Node1(config)# patch wavepatch 2/2/0 filter 0/0/2
Node1(config)# patch wavepatch 2/3/0 filter 0/0/3
Node1(config)# patch wavepatch 2/0/1 filter 1/1/0
Node1(config)# patch wavepatch 2/1/1 filter 1/1/1
Node1(config)# patch wavepatch 2/2/1 filter 1/1/2
Node1(config)# patch wavepatch 2/3/1 filter 1/1/3

Node1(config)# patch wavepatch 3/0/0 filter 0/0/4
  
```

```

Node1(config)# patch wavepatch 3/1/0 filter 0/0/5
Node1(config)# patch wavepatch 3/2/0 filter 0/0/6
Node1(config)# patch wavepatch 3/3/0 filter 0/0/7
Node1(config)# patch wavepatch 3/0/1 filter 1/1/4
Node1(config)# patch wavepatch 3/1/1 filter 1/1/5
Node1(config)# patch wavepatch 3/2/1 filter 1/1/6
Node1(config)# patch wavepatch 3/3/1 filter 1/1/7

Node1(config)# patch wavepatch 4/0/0 filter 0/1/8
Node1(config)# patch wavepatch 4/1/0 filter 0/1/9
Node1(config)# patch wavepatch 4/2/0 filter 0/1/10
Node1(config)# patch wavepatch 4/3/0 filter 0/1/11
Node1(config)# patch wavepatch 4/0/1 filter 1/1/8
Node1(config)# patch wavepatch 4/1/1 filter 1/1/9
Node1(config)# patch wavepatch 4/2/1 filter 1/1/10
Node1(config)# patch wavepatch 4/3/1 filter 1/1/11

Node1(config)# patch wavepatch 5/0/0 filter 0/1/12
Node1(config)# patch wavepatch 5/1/0 filter 0/1/13
Node1(config)# patch wavepatch 5/2/0 filter 0/1/14
Node1(config)# patch wavepatch 5/3/0 filter 0/1/15
Node1(config)# patch wavepatch 5/0/1 filter 1/1/12
Node1(config)# patch wavepatch 5/1/1 filter 1/1/13
Node1(config)# patch wavepatch 5/2/1 filter 1/1/14
Node1(config)# patch wavepatch 5/3/1 filter 1/1/15

```

Transparent Interfaces

```

Node1(config)# interface transparent 2/0/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 2/1/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 2/1
Node1(config-if)# laser frequency 192200
Node1(config-if)# exit

Node1(config)# interface transparent 2/2/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 2/3/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 2/3
Node1(config-if)# laser frequency 192400
Node1(config-if)# exit

Node1(config)# interface transparent 3/0/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 3/1/0
Node1(config-if)# encapsulation gigabitethernet

```



```
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 3/1
Node1(config-if)# laser frequency 192700
Node1(config-if)# exit

Node1(config)# interface transparent 3/2/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 3/3/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 3/3
Node1(config-if)# laser frequency 192900
Node1(config-if)# exit

Node1(config)# interface transparent 4/0/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 4/1/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 4/1
Node1(config-if)# laser frequency 193200
Node1(config-if)# exit

Node1(config)# interface transparent 4/2/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 4/3/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 4/3
Node1(config-if)# laser frequency 193400
Node1(config-if)# exit

Node1(config)# interface transparent 5/0/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 5/1/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 5/1
Node1(config-if)# laser frequency 193700
Node1(config-if)# exit

Node1(config)# interface transparent 5/2/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 5/3/0
```

```

Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 5/3
Node1(config-if)# laser frequency 193900
Node1(config-if)# exit

```

OSC Interfaces

```

Node1(config)# interface wave 0
Node1(config-if)# no shutdown
Node1(config-if)# exit

```

```

Node1(config)# interface wave 1
Node1(config-if)# no shutdown
Node1(config-if)# exit

```

APS

```

Node1(config)# redundancy
Node1(config-red)# associate group wavepatch channel1
Node1(config-red-aps)# aps working wavepatch 2/0/1
Node1(config-red-aps)# aps protection wavepatch 2/0/0
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group wavepatch channe2
Node1(config-red-aps)# aps working wavepatch 2/1/1
Node1(config-red-aps)# aps protection wavepatch 2/1/0
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group wavepatch channel3
Node1(config-red-aps)# aps working wavepatch 2/2/1
Node1(config-red-aps)# aps protection wavepatch 2/2/0
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group wavepatch channel4
Node1(config-red-aps)# aps working wavepatch 2/3/1
Node1(config-red-aps)# aps protection wavepatch 2/3/0
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit

```

```

Node1(config-red)# associate group wavepatch channel5
Node1(config-red-aps)# aps working wavepatch 3/0/1
Node1(config-red-aps)# aps protection wavepatch 3/0/0
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group wavepatch channe6
Node1(config-red-aps)# aps working wavepatch 3/1/1
Node1(config-red-aps)# aps protection wavepatch 3/1/0
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group wavepatch channel7
Node1(config-red-aps)# aps working wavepatch 3/2/1
Node1(config-red-aps)# aps protection wavepatch 3/2/0
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group wavepatch channel8
Node1(config-red-aps)# aps working wavepatch 3/3/1
Node1(config-red-aps)# aps protection wavepatch 3/3/0

```

```
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit

Node1(config-red)# associate group wavepatch channel9
Node1(config-red-aps)# aps working wavepatch 4/0/0
Node1(config-red-aps)# aps protection wavepatch 4/0/1
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group wavepatch channel10
Node1(config-red-aps)# aps working wavepatch 4/1/0
Node1(config-red-aps)# aps protection wavepatch 4/1/1
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group wavepatch channel11
Node1(config-red-aps)# aps working wavepatch 4/2/0
Node1(config-red-aps)# aps protection wavepatch 4/2/1
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group wavepatch channel12
Node1(config-red-aps)# aps working wavepatch 4/3/0
Node1(config-red-aps)# aps protection wavepatch 4/3/1
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit

Node1(config-red)# associate group wavepatch channel13
Node1(config-red-aps)# aps working wavepatch 5/0/0
Node1(config-red-aps)# aps protection wavepatch 5/0/1
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group wavepatch channel14
Node1(config-red-aps)# aps working wavepatch 5/1/0
Node1(config-red-aps)# aps protection wavepatch 5/1/1
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group wavepatch channel15
Node1(config-red-aps)# aps working wavepatch 5/2/0
Node1(config-red-aps)# aps protection wavepatch 5/2/1
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group wavepatch channel16
Node1(config-red-aps)# aps working wavepatch 5/3/0
Node1(config-red-aps)# aps protection wavepatch 5/3/1
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# end

Node1# copy system:running-config nvram:startup-config
```

Node 2

Figure 10-6 shows the shelf configuration for node 2 in the example hubbed ring network shown in Figure 10-3 on page 10-4. A splitter line card motherboard is used in slot 2, and 4-channel mux/demux modules are used in subslot 0 of the west and east mux/demux slots 0 and 1. The line card motherboard cross connects the signal to both mux/demux modules.

Figure 10-6 Shelf Configuration for Node 2 in Splitter Protected Hubbed Ring

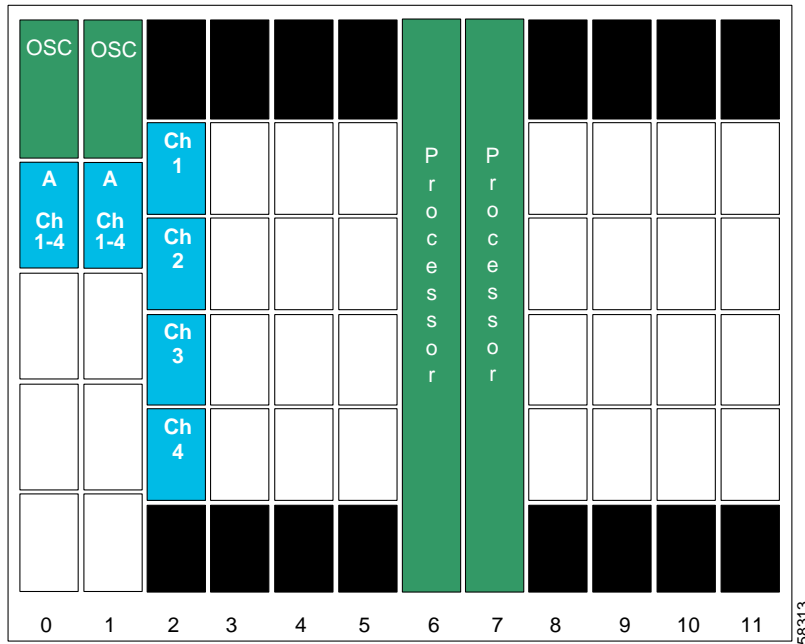
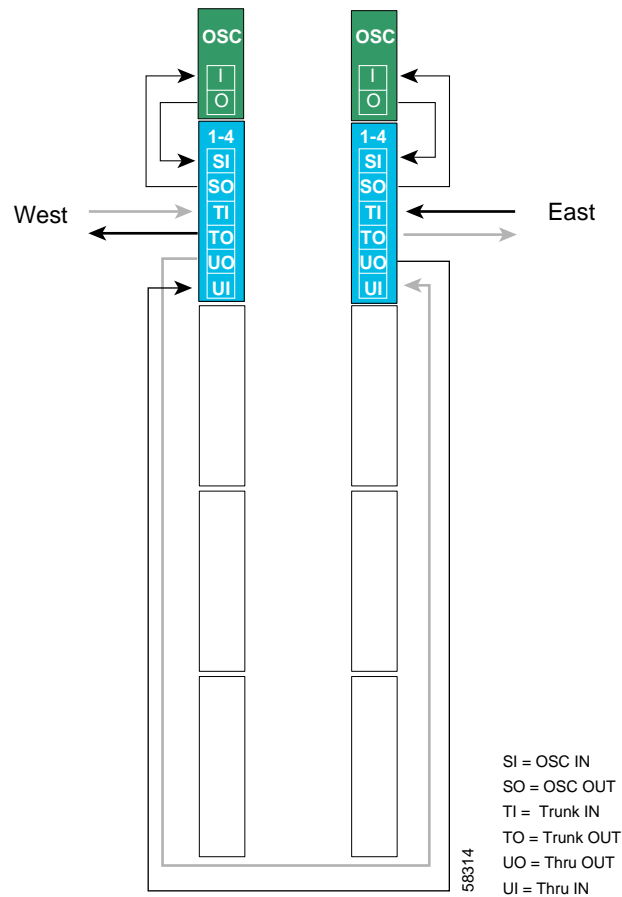


Figure 10-7 shows how the 4-channel mux/demux modules are cabled for node 2 in the splitter protected hubbed ring shown in Figure 10-3 on page 10-4.

Figure 10-7 Add/Drop Mux/Demux Module Cabling with OSC for Node 2 in Splitter Protected Hubbed Ring



Patch Connections

```
Node2# configure terminal
Node2(config)# patch thru 0/0 thru 1/0
Node2(config)# patch wave 0 oscfilter 0/0
Node2(config)# patch wave 1 oscfilter 1/0

Node2(config)# patch wavepatch 2/0/0 filter 0/0/0
Node2(config)# patch wavepatch 2/1/0 filter 0/0/1
Node2(config)# patch wavepatch 2/2/0 filter 0/0/2
Node2(config)# patch wavepatch 2/3/0 filter 0/0/3
Node2(config)# patch wavepatch 2/0/1 filter 1/0/0
Node2(config)# patch wavepatch 2/1/1 filter 1/0/1
Node2(config)# patch wavepatch 2/2/1 filter 1/0/2
Node2(config)# patch wavepatch 2/3/1 filter 1/0/3
```

Transparent Interfaces in Slot 2

```
Node2(config)# interface transparent 2/0/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 2/1/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
Node2(config)# interface wave 2/1
Node2(config-if)# laser frequency 192200
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 2/2/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 2/3/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
Node2(config)# interface wave 2/3
Node2(config-if)# laser frequency 192400
Node2(config-if)# exit
```

OSC Interfaces

```
Node2(config)# interface wave 0
Node2(config-if)# no shutdown
Node2(config-if)# exit
```

```
Node2(config)# interface wave 1
Node2(config-if)# no shutdown
Node2(config-if)# exit
```

APS

```
Node2(config)# redundancy
Node2(config-red)# associate group wavepatch channel1
Node2(config-red-aps)# aps working wavepatch 2/0/0
Node2(config-red-aps)# aps protection wavepatch 2/0/1
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# exit
Node2(config-red)# associate group wavepatch channel2
Node2(config-red-aps)# aps working wavepatch 2/1/0
Node2(config-red-aps)# aps protection wavepatch 2/1/1
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# exit
Node2(config-red)# associate group wavepatch channel3
Node2(config-red-aps)# aps working wavepatch 2/2/0
Node2(config-red-aps)# aps protection wavepatch 2/2/1
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# exit
Node2(config-red)# associate group wavepatch channel4
Node2(config-red-aps)# aps working wavepatch 2/3/0
Node2(config-red-aps)# aps protection wavepatch 2/3/1
```

```

Node2(config-red-aps)# aps enable
Node2(config-red-aps)# end

Node2# copy system:running-config nvram:startup-config

```

Node 3

Figure 10-8 shows the shelf configuration for node 3 in the example hubbed ring network shown in Figure 10-3 on page 10-4. A splitter line card motherboard is used in slot 5, and 4-channel mux/demux modules are used in subslot 1 of the west and east mux/demux slots 0 and 1. The line card motherboard cross connects the signal to both mux/demux modules.

Figure 10-8 Shelf Configuration for Node 3 in Splitter Protected Hubbed Ring

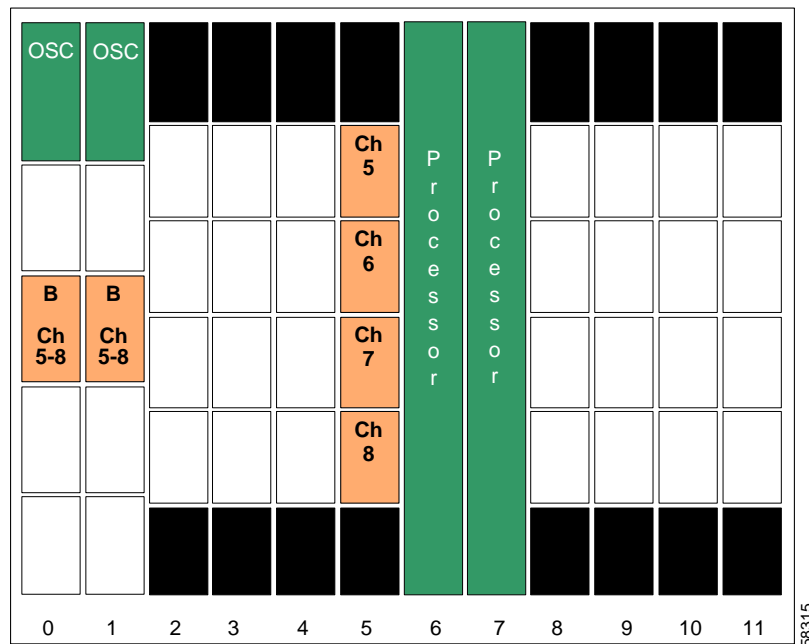
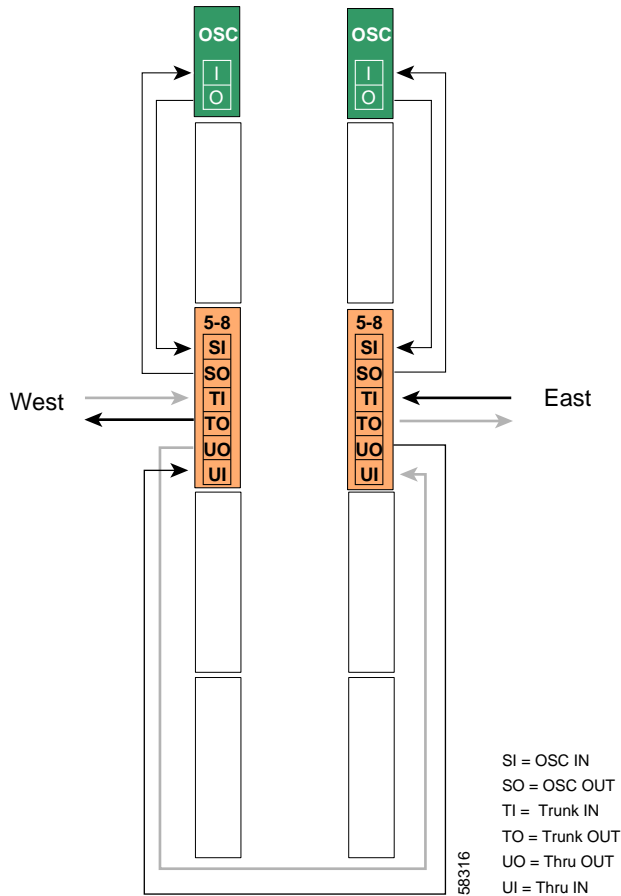


Figure 10-9 shows how the 4-channel mux/demux modules are cabled for node 3 in the splitter protected hubbed ring network shown in Figure 10-3 on page 10-4.

Figure 10-9 Add/Drop Mux/Demux Module Cabling with OSC for Node 3 in Splitter Protected Hubbed Ring



Patch Connections

```

Node3# configure terminal
Node3 (config)# patch thru 0/1 thru 1/1
Node3 (config)# patch wave 0 oscfilter 0/1
Node3 (config)# patch wave 1 oscfilter 1/1

Node3 (config)# patch wavepatch 4/0/0 filter 0/1/0
Node3 (config)# patch wavepatch 4/1/0 filter 0/1/1
Node3 (config)# patch wavepatch 4/2/0 filter 0/1/2
Node3 (config)# patch wavepatch 4/3/0 filter 0/1/3
Node3 (config)# patch wavepatch 4/0/1 filter 1/1/0
Node3 (config)# patch wavepatch 4/1/1 filter 1/1/1
Node3 (config)# patch wavepatch 4/2/1 filter 1/1/2
Node3 (config)# patch wavepatch 4/3/1 filter 1/1/3
  
```

Transparent Interfaces in Slot 4

```

Node3 (config)# interface transparent 4/0/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
  
```



```

Node3(config-if)# exit

Node3(config)# interface transparent 4/1/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
Node3(config)# interface wave 4/1
Node3(config-if)# laser frequency 193200
Node3(config-if)# exit

Node3(config)# interface transparent 4/2/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit

Node3(config)# interface transparent 4/3/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
Node3(config)# interface wave 4/3
Node3(config-if)# laser frequency 193400
Node3(config-if)# exit

```

OSC Interfaces

```

Node3(config)# interface wave 0
Node3(config-if)# no shutdown
Node3(config-if)# exit

Node3(config)# interface wave 1
Node3(config-if)# no shutdown
Node3(config-if)# exit

```

APS

```

Node3(config)# redundancy
Node3(config-red)# associate group wavepatch channel5
Node3(config-red-aps)# aps working wavepatch 5/0/0
Node3(config-red-aps)# aps protection wavepatch 5/0/1
Node3(config-red-aps)# aps enable
Node3(config-red-aps)# exit
Node3(config-red)# associate group wavepatch channel6
Node3(config-red-aps)# aps working wavepatch 5/1/0
Node3(config-red-aps)# aps protection wavepatch 5/1/1
Node3(config-red-aps)# aps enable
Node3(config-red-aps)# exit
Node3(config-red)# associate group wavepatch channel7
Node3(config-red-aps)# aps working wavepatch 5/2/0
Node3(config-red-aps)# aps protection wavepatch 5/2/1
Node3(config-red-aps)# aps enable
Node3(config-red-aps)# exit
Node3(config-red)# associate group wavepatch channel8
Node3(config-red-aps)# aps working wavepatch 5/3/0
Node3(config-red-aps)# aps protection wavepatch 5/3/1
Node3(config-red-aps)# aps enable
Node3(config-red-aps)# end

Node3# copy system:running-config nvram:startup-config

```

Node 4

Figure 10-10 shows the shelf configuration for node 4 in the hubbed ring network shown in Figure 10-3 on page 10-4. A splitter line card motherboard is used in slot 8, and 4-channel mux/demux modules are used in subslot 2 of the west and east mux/demux slots 0 and 1. The line card motherboard cross connects the signal to both mux/demux modules.

Figure 10-10 Shelf Configuration for Node 4 in Splitter Protected Hubbed Ring

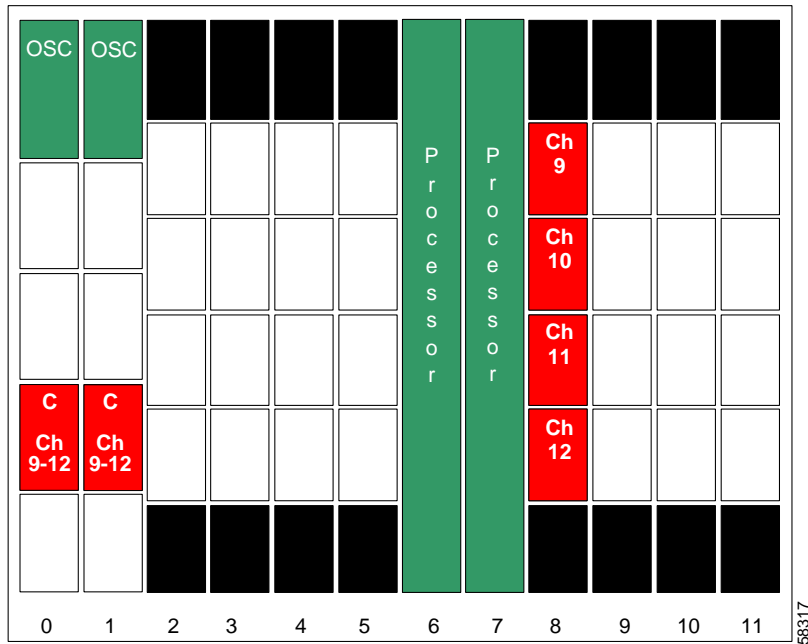
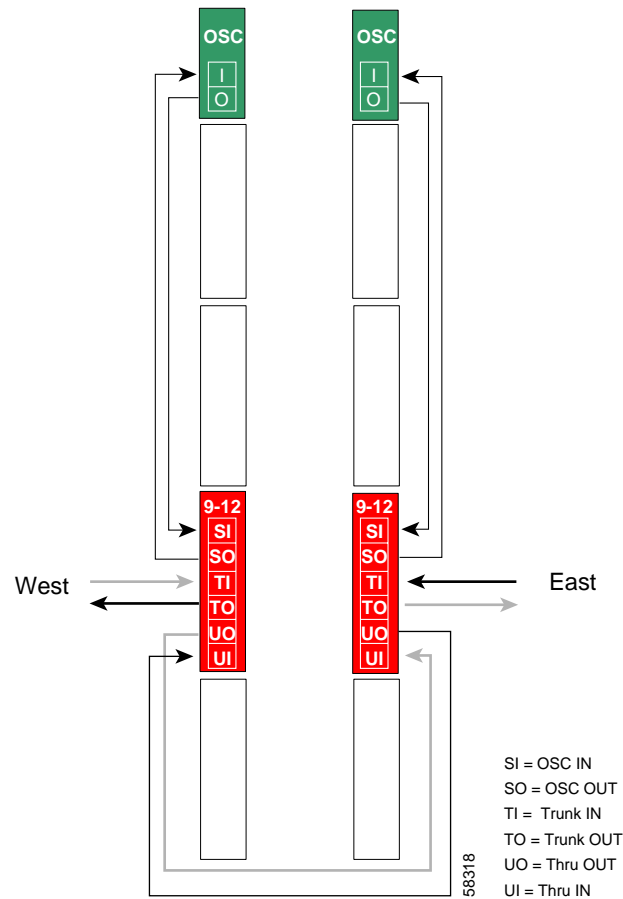


Figure 10-11 shows how the 4-channel mux/demux modules are cabled for node 4 in the splitter protected hubbed ring network shown in Figure 10-3 on page 10-4.

Figure 10-11 Add/Drop Mux/Demux Module Cabling with OSC for Node 4 in Splitter Protected Hubbed Ring



Patch Connections

```

Node4# configure terminal
Node4(config)# patch thru 0/2 thru 1/2
Node4(config)# patch wave 0 oscfilter 0/2
Node4(config)# patch wave 1 oscfilter 1/2

Node4(config)# patch wavepatch 8/0/0 filter 0/2/0
Node4(config)# patch wavepatch 8/1/0 filter 0/2/1
Node4(config)# patch wavepatch 8/2/0 filter 0/2/2
Node4(config)# patch wavepatch 8/3/0 filter 0/2/3
Node4(config)# patch wavepatch 8/0/1 filter 1/2/0
Node4(config)# patch wavepatch 8/1/1 filter 1/2/1
Node4(config)# patch wavepatch 8/2/1 filter 1/2/2
Node4(config)# patch wavepatch 8/3/1 filter 1/2/3
  
```

Transparent Interfaces in Slot 8

```
Node4 (config)# interface transparent 8/0/0
Node4 (config-if)# encapsulation gigabitethernet
Node4 (config-if)# monitor enable
Node4 (config-if)# exit
```

```
Node4 (config)# interface transparent 8/1/0
Node4 (config-if)# encapsulation gigabitethernet
Node4 (config-if)# monitor enable
Node4 (config-if)# exit
Node4 (config)# interface wave 8/1
Node4 (config-if)# laser frequency 194200
Node4 (config-if)# exit
```

```
Node4 (config)# interface transparent 8/2/0
Node4 (config-if)# encapsulation gigabitethernet
Node4 (config-if)# monitor enable
Node4 (config-if)# exit
```

```
Node4 (config)# interface transparent 8/3/0
Node4 (config-if)# encapsulation gigabitethernet
Node4 (config-if)# monitor enable
Node4 (config-if)# exit
Node4 (config)# interface wave 8/3
Node4 (config-if)# laser frequency 194400
Node4 (config-if)# exit
```

OSC Interfaces

```
Node4 (config)# interface wave 0
Node4 (config-if)# no shutdown
Node4 (config-if)# exit
```

```
Node4 (config)# interface wave 1
Node4 (config-if)# no shutdown
Node4 (config-if)# exit
```

APS

```
Node4 (config)# redundancy
Node4 (config-red)# associate group channel9
Node4 (config-red-aps)# aps working wavepatch 8/0/1
Node4 (config-red-aps)# aps protection wavepatch 8/0/0
Node4 (config-red-aps)# aps enable
Node4 (config-red-aps)# exit
Node4 (config-red)# associate group channel10
Node4 (config-red-aps)# aps working wavepatch 8/1/1
Node4 (config-red-aps)# aps protection wavepatch 8/1/0
Node4 (config-red-aps)# aps enable
Node4 (config-red-aps)# exit
Node4 (config-red)# associate group channel11
Node4 (config-red-aps)# aps working wavepatch 8/2/1
Node4 (config-red-aps)# aps protection wavepatch 8/2/0
Node4 (config-red-aps)# aps enable
Node4 (config-red-aps)# exit
Node4 (config-red)# associate group channel12
Node4 (config-red-aps)# aps working wavepatch 8/3/1
Node4 (config-red-aps)# aps protection wavepatch 8/3/0
```

```
Node4(config-red-aps)# aps enable
Node4(config-red-aps)# exit
Node4(config-red-aps)# end

Node4# copy system:running-config nvram:startup-config
```

Node 5

Figure 10-12 shows the shelf configuration for node 5 in the example network shown in Figure 10-3 on page 10-4. A splitter line card motherboard is used in slot 11, and 4-channel mux/demux modules are used in subslot 3 of the west and east mux/demux slots 0 and 1. The line card motherboard cross connects the signal to both mux/demux modules.

Figure 10-12 Shelf Configuration for Node 5 in Splitter Protected Hubbed Ring

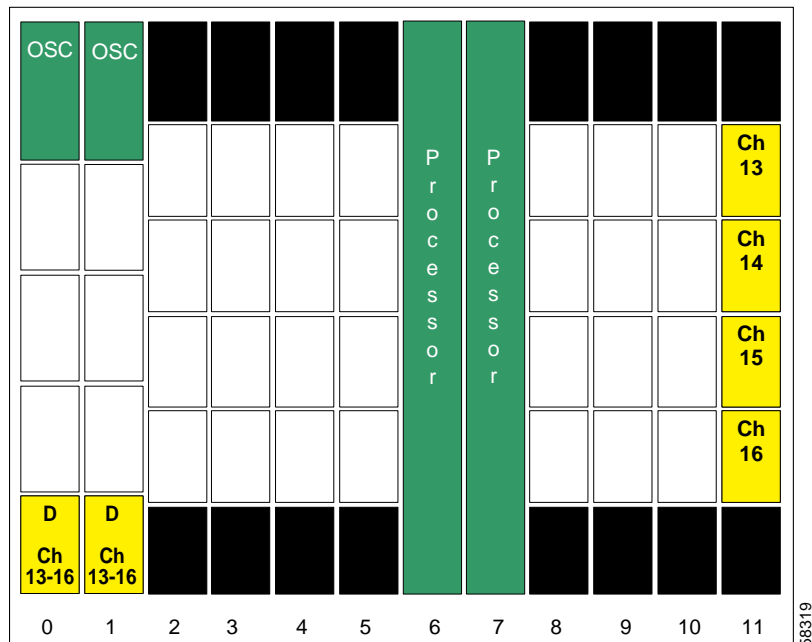
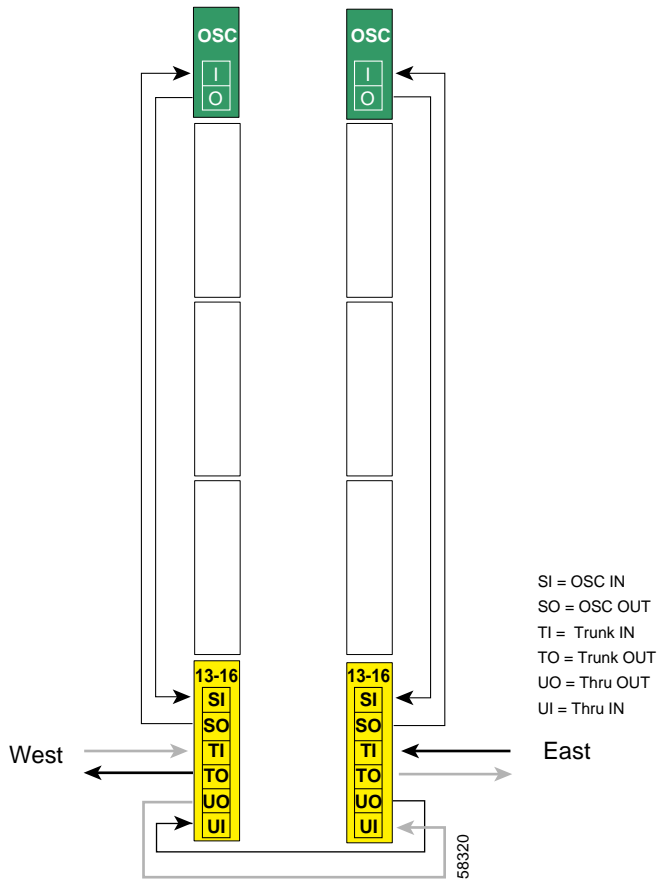


Figure 10-13 shows how the 4-channel mux/demux modules are cabled for node 5 in the example network shown in Figure 10-3 on page 10-4.

Figure 10-13 Add/Drop Mux/Demux Module Cabling with OSC for Node 5 in Splitter Protected Hubbed Ring



Patch Connections

```

Node5# configure terminal
Node5(config)# patch thru 0/3 thru 1/3
Node5(config)# patch wave 0 oscfilter 0/3
Node5(config)# patch wave 1 oscfilter 1/3

Node5(config)# patch wavepatch 11/0/0 filter 0/3/0
Node5(config)# patch wavepatch 11/1/0 filter 0/3/1
Node5(config)# patch wavepatch 11/2/0 filter 0/3/2
Node5(config)# patch wavepatch 11/3/0 filter 0/3/3
Node5(config)# patch wavepatch 11/0/1 filter 1/3/0
Node5(config)# patch wavepatch 11/1/1 filter 1/3/1
Node5(config)# patch wavepatch 11/2/1 filter 1/3/2
Node5(config)# patch wavepatch 11/3/1 filter 1/3/3
  
```

Transparent Interfaces in Slot 11

```

Node5(config)# interface transparent 11/0/0
Node5(config-if)# encapsulation gigabitethernet
Node5(config-if)# monitor enable
  
```

```

Node5(config-if)# exit

Node5(config)# interface transparent 11/1/0
Node5(config-if)# encapsulation gigabitethernet
Node5(config-if)# monitor enable
Node5(config-if)# exit
Node5(config)# interface wave 11/1
Node5(config-if)# laser frequency 195700
Node5(config-if)# exit

Node5(config)# interface transparent 11/2/0
Node5(config-if)# encapsulation gigabitethernet
Node5(config-if)# monitor enable
Node5(config-if)# exit

Node5(config)# interface transparent 11/3/0
Node5(config-if)# encapsulation gigabitethernet
Node5(config-if)# monitor enable
Node5(config-if)# exit
Node5(config)# interface wave 11/3
Node5(config-if)# laser frequency 195900
Node5(config-if)# exit

```

OSC Interfaces

```

Node5(config)# interface wave 0
Node5(config-if)# no shutdown
Node5(config-if)# exit

Node5(config)# interface wave 1
Node5(config-if)# no shutdown
Node5(config-if)# exit

```

APS

```

Node5(config)# redundancy
Node5(config-red)# associate group channel13
Node5(config-red-aps)# aps working wavepatch 11/0/1
Node5(config-red-aps)# aps protection wavepatch 11/0/0
Node5(config-red-aps)# aps enable
Node5(config-red-aps)# exit
Node5(config-red)# associate group channel14
Node5(config-red-aps)# aps working wavepatch 11/1/1
Node5(config-red-aps)# aps protection wavepatch 11/1/0
Node5(config-red-aps)# aps enable
Node5(config-red-aps)# exit
Node5(config-red)# associate group channel15
Node5(config-red-aps)# aps working wavepatch 11/2/1
Node5(config-red-aps)# aps protection wavepatch 11/2/0
Node5(config-red-aps)# aps enable
Node5(config-red-aps)# exit
Node5(config-red)# associate group channel16
Node5(config-red-aps)# aps working wavepatch 11/3/1
Node5(config-red-aps)# aps protection wavepatch 11/3/0
Node5(config-red-aps)# aps enable
Node5(config-red-aps)# exit
Node5(config-red-aps)# end

Node5# copy system:running-config nvram:startup-config

```

Configuring a Hubbed Ring with Line Card Protection and OSC

Line card protection requires a different shelf and CLI configuration from splitter protection. The following sections describe an example based on the hubbed ring topology shown in Figure 10-3 on page 10-4.


Note

For information about configuring nodes with more than 16 channels and line card protection, see Chapter 8, “Configuring Dual Shelf Nodes.”

Node 1

Figure 10-14 shows the shelf configuration for the hub node in the hubbed ring example shown in Figure 10-3 on page 10-4. The line card motherboards in slots 2–5 are unprotected motherboards that cross connect the signal to the 8-channel mux/demux module in the west mux/demux slot 0; the line card motherboards in slots 8–11 are unprotected motherboards that cross connect the signal to the 8-channel mux/demux module in the east mux/demux slot 1.

Figure 10-14 Shelf Configuration for Hub Node in Line Card Protected Hubbed Ring

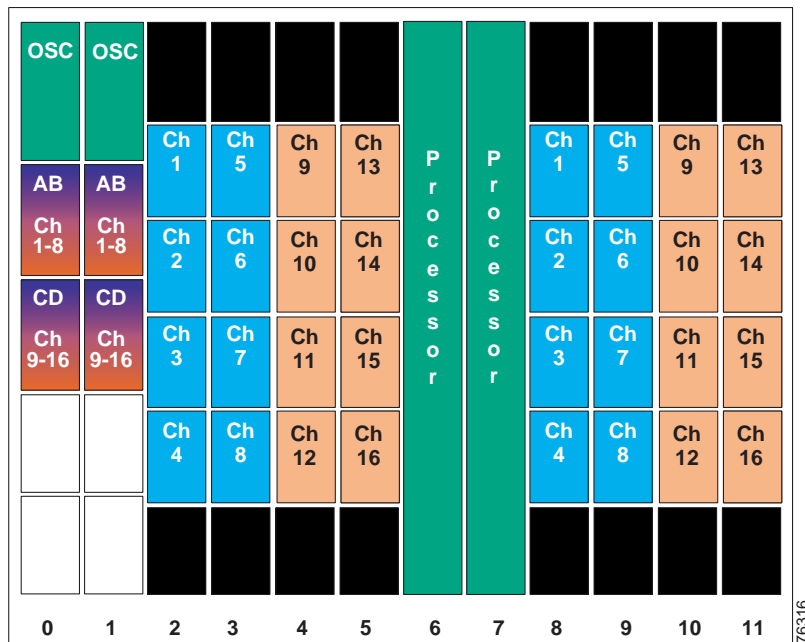
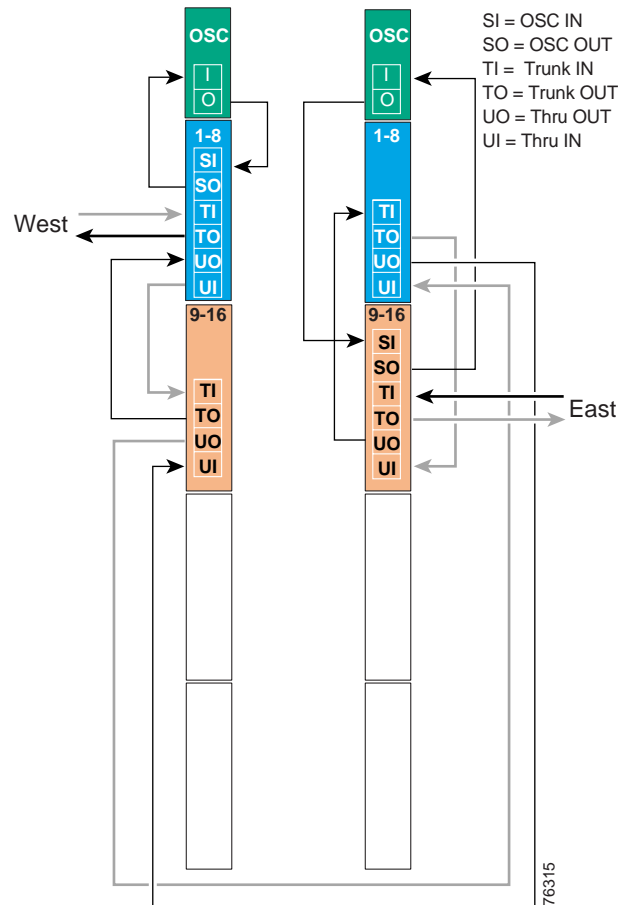


Figure 10-15 shows how the 8-channel mux/demux modules are cabled for node 1 in the hub node in the line card protected hubbed ring shown in Figure 10-3 on page 10-4.

Figure 10-15 Terminal Mux/Demux Module Cabling with OSC for Hub Node in Line Card Protected Hubbed Ring



Patch Connections

```

Node1# configure terminal
Node1(config)# patch wave 0 oscfilter 0/0
Node1(config)# patch wave 1 oscfilter 1/1

Node1(config)# patch thru 0/0 wdm 0/1
Node1(config)# patch thru 0/1 thru 1/0
Node1(config)# patch wdm 1/0 thru 1/1

Node1(config)# patch wavepatch 2/0/0 filter 0/0/0
Node1(config)# patch wavepatch 2/1/0 filter 0/0/1
Node1(config)# patch wavepatch 2/2/0 filter 0/0/2
Node1(config)# patch wavepatch 2/3/0 filter 0/0/3

Node1(config)# patch wavepatch 3/0/0 filter 0/0/4
Node1(config)# patch wavepatch 3/1/0 filter 0/0/5
Node1(config)# patch wavepatch 3/2/0 filter 0/0/6

```

```

Node1(config)# patch wavepatch 3/3/0 filter 0/0/7

Node1(config)# patch wavepatch 4/0/0 filter 0/1/8
Node1(config)# patch wavepatch 4/1/0 filter 0/1/9
Node1(config)# patch wavepatch 4/2/0 filter 0/1/10
Node1(config)# patch wavepatch 4/3/0 filter 0/1/11

Node1(config)# patch wavepatch 5/0/0 filter 0/1/12
Node1(config)# patch wavepatch 5/1/0 filter 0/1/13
Node1(config)# patch wavepatch 5/2/0 filter 0/1/14
Node1(config)# patch wavepatch 5/3/0 filter 0/1/15

Node1(config)# patch wavepatch 8/0/0 filter 1/0/0
Node1(config)# patch wavepatch 8/1/0 filter 1/0/1
Node1(config)# patch wavepatch 8/2/0 filter 1/0/2
Node1(config)# patch wavepatch 8/3/0 filter 1/0/3

Node1(config)# patch wavepatch 9/0/0 filter 1/0/4
Node1(config)# patch wavepatch 9/1/0 filter 1/0/5
Node1(config)# patch wavepatch 9/2/0 filter 1/0/6
Node1(config)# patch wavepatch 9/3/0 filter 1/0/7

Node1(config)# patch wavepatch 10/0/0 filter 1/1/8
Node1(config)# patch wavepatch 10/1/0 filter 1/1/9
Node1(config)# patch wavepatch 10/2/0 filter 1/1/10
Node1(config)# patch wavepatch 10/3/0 filter 1/1/11

Node1(config)# patch wavepatch 11/0/0 filter 1/1/12
Node1(config)# patch wavepatch 11/1/0 filter 1/1/13
Node1(config)# patch wavepatch 11/2/0 filter 1/1/14
Node1(config)# patch wavepatch 11/3/0 filter 1/1/15

```

Transparent Interfaces

```

Node1(config)# interface transparent 2/0/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 2/1/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 2/1
Node1(config-if)# laser frequency 192200
Node1(config-if)# exit

Node1(config)# interface transparent 2/2/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 2/3/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 2/3
Node1(config-if)# laser frequency 192400
Node1(config-if)# exit

Node1(config)# interface transparent 3/0/0

```

```
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 3/1/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 3/1
Node1(config-if)# laser frequency 192700
Node1(config-if)# exit

Node1(config)# interface transparent 3/2/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 3/3/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 3/3
Node1(config-if)# laser frequency 192900
Node1(config-if)# exit

Node1(config)# interface transparent 4/0/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 4/1/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 4/1
Node1(config-if)# laser frequency 193200
Node1(config-if)# exit

Node1(config)# interface transparent 4/2/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 4/3/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 4/3
Node1(config-if)# laser frequency 193400
Node1(config-if)# exit

Node1(config)# interface transparent 5/0/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 5/1/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 5/1
Node1(config-if)# laser frequency 193700
Node1(config-if)# exit
```

```
Node1(config)# interface transparent 5/2/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
```

```
Node1(config)# interface transparent 5/3/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 5/3
Node1(config-if)# laser frequency 193900
Node1(config-if)# exit
```

```
Node1(config)# interface transparent 8/0/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
```

```
Node1(config)# interface transparent 8/1/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 8/1
Node1(config-if)# laser frequency 192200
Node1(config-if)# exit
```

```
Node1(config)# interface transparent 8/2/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
```

```
Node1(config)# interface transparent 8/3/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 8/3
Node1(config-if)# laser frequency 192400
Node1(config-if)# exit
```

```
Node1(config)# interface transparent 9/0/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
```

```
Node1(config)# interface transparent 9/1/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 9/1
Node1(config-if)# laser frequency 192700
Node1(config-if)# exit
```

```
Node1(config)# interface transparent 9/2/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
```

```
Node1(config)# interface transparent 9/3/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 9/3
Node1(config-if)# laser frequency 192900
Node1(config-if)# exit
```

```
Node1(config)# interface transparent 10/0/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 10/1/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 10/1
Node1(config-if)# laser frequency 193200
Node1(config-if)# exit

Node1(config)# interface transparent 10/2/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 10/3/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 10/3
Node1(config-if)# laser frequency 193400
Node1(config-if)# exit

Node1(config)# interface transparent 11/0/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 11/1/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 11/1
Node1(config-if)# laser frequency 1953700
Node1(config-if)# exit

Node1(config)# interface transparent 11/2/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 11/3/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 11/3
Node1(config-if)# laser frequency 193900
Node1(config-if)# exit
```

OSC Interfaces

```
Node1(config)# interface wave 0
Node1(config-if)# no shutdown
Node1(config-if)# exit

Node1(config)# interface wave 1
Node1(config-if)# no shutdown
Node1(config-if)# exit
```

APS

Use the following for configuring y-cable protection.

```

Node1 (config)# redundancy
Node1 (config-red)# associate group channel1
Node1 (config-red-aps)# aps working transparent 8/0/0
Node1 (config-red-aps)# aps protection transparent 2/0/0
Node1 (config-red-aps)# aps y-cable
Node1 (config-red-aps)# aps revertive
Node1 (config-red-aps)# aps enable
Node1 (config-red-aps)# exit
Node1 (config-red)# associate group channel2
Node1 (config-red-aps)# aps working transparent 8/1/0
Node1 (config-red-aps)# aps protection transparent 2/1/0
Node1 (config-red-aps)# aps y-cable
Node1 (config-red-aps)# aps revertive
Node1 (config-red-aps)# aps enable
Node1 (config-red-aps)# exit
Node1 (config-red)# associate group channel3
Node1 (config-red-aps)# aps working transparent 8/2/0
Node1 (config-red-aps)# aps protection transparent 2/2/0
Node1 (config-red-aps)# aps y-cable
Node1 (config-red-aps)# aps revertive
Node1 (config-red-aps)# aps enable
Node1 (config-red-aps)# exit
Node1 (config-red)# associate group channel4
Node1 (config-red-aps)# aps working transparent 8/3/0
Node1 (config-red-aps)# aps protection transparent 2/3/0
Node1 (config-red-aps)# aps y-cable
Node1 (config-red-aps)# aps revertive
Node1 (config-red-aps)# aps enable
Node1 (config-red-aps)# exit

Node1 (config-red)# associate group channel5
Node1 (config-red-aps)# aps working transparent 9/0/0
Node1 (config-red-aps)# aps protection transparent 3/0/0
Node1 (config-red-aps)# aps y-cable
Node1 (config-red-aps)# aps revertive
Node1 (config-red-aps)# aps enable
Node1 (config-red-aps)# exit
Node1 (config-red)# associate group channel6
Node1 (config-red-aps)# aps working transparent 9/1/0
Node1 (config-red-aps)# aps protection transparent 3/1/0
Node1 (config-red-aps)# aps y-cable
Node1 (config-red-aps)# aps revertive
Node1 (config-red-aps)# aps enable
Node1 (config-red-aps)# exit
Node1 (config-red)# associate group channel7
Node1 (config-red-aps)# aps working transparent 9/2/0
Node1 (config-red-aps)# aps protection transparent 3/2/0
Node1 (config-red-aps)# aps y-cable
Node1 (config-red-aps)# aps revertive
Node1 (config-red-aps)# aps enable
Node1 (config-red-aps)# exit
Node1 (config-red)# associate group channel8
Node1 (config-red-aps)# aps working transparent 9/3/0
Node1 (config-red-aps)# aps protection transparent 3/3/0
Node1 (config-red-aps)# aps y-cable
Node1 (config-red-aps)# aps revertive
Node1 (config-red-aps)# aps enable
Node1 (config-red-aps)# exit

```

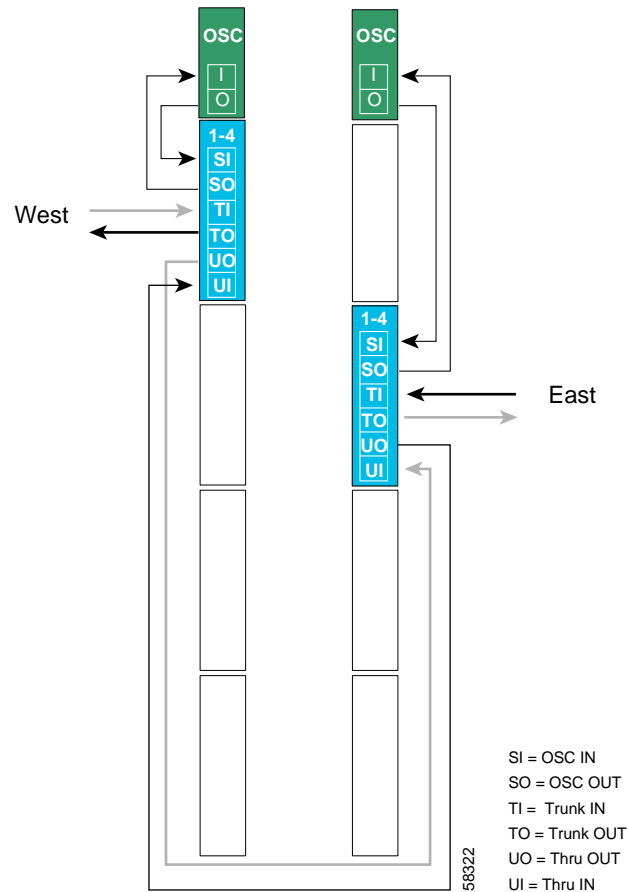
```
Node1(config-red)# associate group channel9
Node1(config-red-aps)# aps working transparent 4/0/0
Node1(config-red-aps)# aps protection transparent 10/0/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps revertive
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel10
Node1(config-red-aps)# aps working transparent 4/1/0
Node1(config-red-aps)# aps protection transparent 10/1/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps revertive
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel11
Node1(config-red-aps)# aps working transparent 4/2/0
Node1(config-red-aps)# aps protection transparent 10/2/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps revertive
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel12
Node1(config-red-aps)# aps working transparent 4/3/0
Node1(config-red-aps)# aps protection transparent 10/3/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps revertive
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit

Node1(config-red)# associate group channel13
Node1(config-red-aps)# aps working transparent 5/0/0
Node1(config-red-aps)# aps protection transparent 11/0/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps revertive
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel14
Node1(config-red-aps)# aps working transparent 5/1/0
Node1(config-red-aps)# aps protection transparent 11/1/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps revertive
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel15
Node1(config-red-aps)# aps working transparent 5/2/0
Node1(config-red-aps)# aps protection transparent 11/2/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps revertive
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel16
Node1(config-red-aps)# aps working transparent 5/3/0
Node1(config-red-aps)# aps protection transparent 11/3/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps revertive
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# end

Node1# copy system:running-config nvram:startup-config
```


Figure 10-17 shows how the 4-channel mux/demux modules are cabled for node 2 in the line card protected hubbed ring shown in Figure 10-3 on page 10-4.

Figure 10-17 Add/Drop Mux/Demux Module Cabling with OSC for Node 2 in Line Card Protected Hubbed Ring



Patch Connections

```
Node2# configure terminal
Node2(config)# patch thru 0/0 thru 1/1
Node2(config)# patch wave 0 oscfilter 0/0
Node2(config)# patch wave 1 oscfilter 1/1

Node2(config)# patch wavepatch 2/0/0 filter 0/0/0
Node2(config)# patch wavepatch 2/1/0 filter 0/0/1
Node2(config)# patch wavepatch 2/2/0 filter 0/0/2
Node2(config)# patch wavepatch 2/3/0 filter 0/0/3

Node2(config)# patch wavepatch 4/0/0 filter 1/1/0
Node2(config)# patch wavepatch 4/1/0 filter 1/1/1
Node2(config)# patch wavepatch 4/2/0 filter 1/1/2
Node2(config)# patch wavepatch 4/3/0 filter 1/1/3
```

Transparent Interfaces in Slot 2

```
Node2(config)# interface transparent 2/0/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 2/1/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
Node2(config)# interface wave 2/1
Node2(config-if)# laser frequency 192200
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 2/2/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 2/3/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
Node2(config)# interface wave 2/3
Node2(config-if)# laser frequency 192400
Node2(config-if)# exit
```

Transparent Interfaces in Slot 4

```
Node2(config)# interface transparent 4/0/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 4/1/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
Node2(config)# interface wave 4/1
Node2(config-if)# laser frequency 192200
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 4/2/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 4/3/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
Node2(config)# interface wave 4/3
Node2(config-if)# laser frequency 192400
Node2(config-if)# exit
```

OSC Interfaces

```
Node2(config)# interface wave 0
Node2(config-if)# no shutdown
```

```
Node2(config-if)# exit

Node2(config)# interface wave 1
Node2(config-if)# no shutdown
Node2(config-if)# exit
```

APS

Use the following for configuring y-cable protection.

```
Node2(config)# redundancy
Node2(config-red)# associate group channel1
Node2(config-red-aps)# aps working transparent 2/0/0
Node2(config-red-aps)# aps protection transparent 4/0/0
Node2(config-red-aps)# aps y-cable
Node2(config-red-aps)# aps revertive
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# exit
Node2(config-red)# associate group channel2
Node2(config-red-aps)# aps working transparent 2/1/0
Node2(config-red-aps)# aps protection transparent 4/1/0
Node2(config-red-aps)# aps y-cable
Node2(config-red-aps)# aps revertive
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# exit
Node2(config-red)# associate group channel3
Node2(config-red-aps)# aps working transparent 2/2/0
Node2(config-red-aps)# aps protection transparent 4/2/0
Node2(config-red-aps)# aps y-cable
Node2(config-red-aps)# aps revertive
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# exit
Node2(config-red)# associate group channel4
Node2(config-red-aps)# aps working transparent 2/3/0
Node2(config-red-aps)# aps protection transparent 4/3/0
Node2(config-red-aps)# aps y-cable
Node2(config-red-aps)# aps revertive
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# end

Node2# copy system:running-config nvram:startup-config
```

Node 3

Figure 10-18 shows the shelf configuration for node 3 in the line card protected hubbed ring shown in Figure 10-3 on page 10-4. Slot 3 uses a nonsplitter line card motherboard, that cross connects the signal to the add/drop mux/demux module in the east mux/demux slot 1; slot 5 uses a nonsplitter line card motherboard that cross connects the signal to the add/drop mux/demux module in the west mux/demux slot 0.

Figure 10-18 Shelf Configuration for Node 3 in Line Card Protected Hubbed Ring

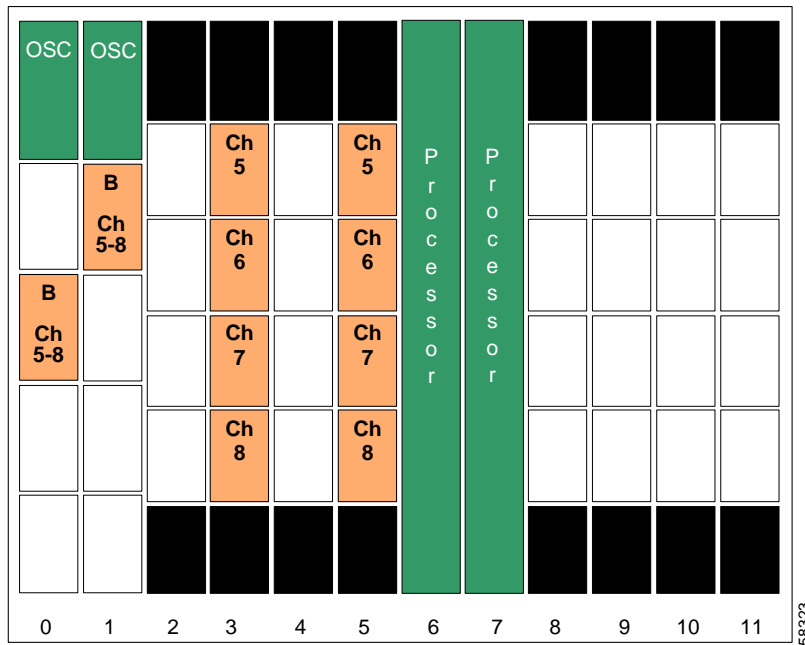
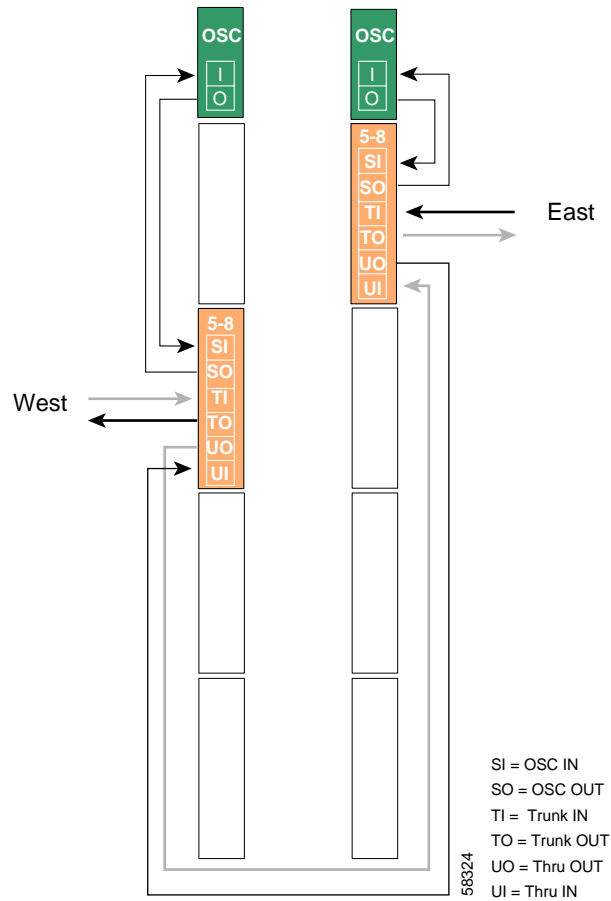


Figure 10-19 shows how the 4-channel mux/demux modules are cabled for node 3 in the line card protected hubbed ring shown in Figure 10-3 on page 10-4.

Figure 10-19 Add/Drop Mux/Demux Module Cabling with OSC for Node 3 in Line Card Protected Hubbed Ring



Patch Connections

```
Node3# configure terminal
Node3(config)# patch thru 0/1 thru 1/0
Node3(config)# patch wave 0 oscfilter 0/1
Node3(config)# patch wave 1 oscfilter 1/0

Node3(config)# patch wavepatch 3/0/0 filter 0/1/0
Node3(config)# patch wavepatch 3/1/0 filter 0/1/1
Node3(config)# patch wavepatch 3/2/0 filter 0/1/2
Node3(config)# patch wavepatch 3/3/0 filter 0/1/3

Node3(config)# patch wavepatch 5/0/0 filter 1/0/0
Node3(config)# patch wavepatch 5/1/0 filter 1/0/1
Node3(config)# patch wavepatch 5/2/0 filter 1/0/2
Node3(config)# patch wavepatch 5/3/0 filter 1/0/3
```

Transparent Interfaces in Slot 3

```
Node3 (config)# interface transparent 3/0/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit
```

```
Node3 (config)# interface transparent 3/1/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit
Node3 (config)# interface wave 3/1
Node3 (config-if)# laser frequency 192700
Node3 (config-if)# exit
```

```
Node3 (config)# interface transparent 3/2/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit
```

```
Node3 (config)# interface transparent 3/3/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit
Node3 (config)# interface wave 3/3
Node3 (config-if)# laser frequency 192900
Node3 (config-if)# exit
```

Transparent Interfaces in Slot 5

```
Node3 (config)# interface transparent 5/0/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit
```

```
Node3 (config)# interface transparent 5/1/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit
Node3 (config)# interface wave 5/1
Node3 (config-if)# laser frequency 192700
Node3 (config-if)# exit
```

```
Node3 (config)# interface transparent 5/2/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit
```

```
Node3 (config)# interface transparent 5/3/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit
Node3 (config)# interface wave 5/3
Node3 (config-if)# laser frequency 192900
Node3 (config-if)# exit
```

OSC Interfaces

```
Node3 (config)# interface wave 0
```

```
Node3(config-if)# no shutdown
Node3(config-if)# exit

Node3(config)# interface wave 1
Node3(config-if)# no shutdown
Node3(config-if)# exit
```

APS

Use the following for configuring y-cable protection.

```
Node3(config)# redundancy
Node3(config-red)# associate group channel5
Node3(config-red-aps)# aps working transparent 5/0/0
Node3(config-red-aps)# aps protection transparent 3/0/0
Node3(config-red-aps)# aps y-cable
Node3(config-red-aps)# aps revertive
Node3(config-red-aps)# aps enable
Node3(config-red-aps)# exit
Node3(config-red)# associate group channel6
Node3(config-red-aps)# aps working transparent 5/1/0
Node3(config-red-aps)# aps protection transparent 3/1/0
Node3(config-red-aps)# aps y-cable
Node3(config-red-aps)# aps revertive
Node3(config-red-aps)# aps enable
Node3(config-red-aps)# exit
Node3(config-red)# associate group channel7
Node3(config-red-aps)# aps working transparent 5/2/0
Node3(config-red-aps)# aps protection transparent 3/2/0
Node3(config-red-aps)# aps y-cable
Node3(config-red-aps)# aps revertive
Node3(config-red-aps)# aps enable
Node3(config-red-aps)# exit
Node3(config-red)# associate group channel8
Node3(config-red-aps)# aps working transparent 5/3/0
Node3(config-red-aps)# aps protection transparent 3/3/0
Node3(config-red-aps)# aps y-cable
Node3(config-red-aps)# aps revertive
Node3(config-red-aps)# aps enable
Node3(config-red-aps)# end

Node3# copy system:running-config nvram:startup-config
```

Node 4

Figure 10-20 shows the shelf configuration for node 4 in the line card protected hubbed ring shown in Figure 10-3 on page 10-4. Slot 8 uses a nonsplitter line card motherboard that cross connects the signal to the add/drop mux/demux module in the west mux/demux slot 0; slot 10 uses a nonsplitter line card motherboard that cross connects the signal to the add/drop mux/demux module in the east mux/demux slot 1.

Figure 10-20 Module Installation Configuration for Node 4

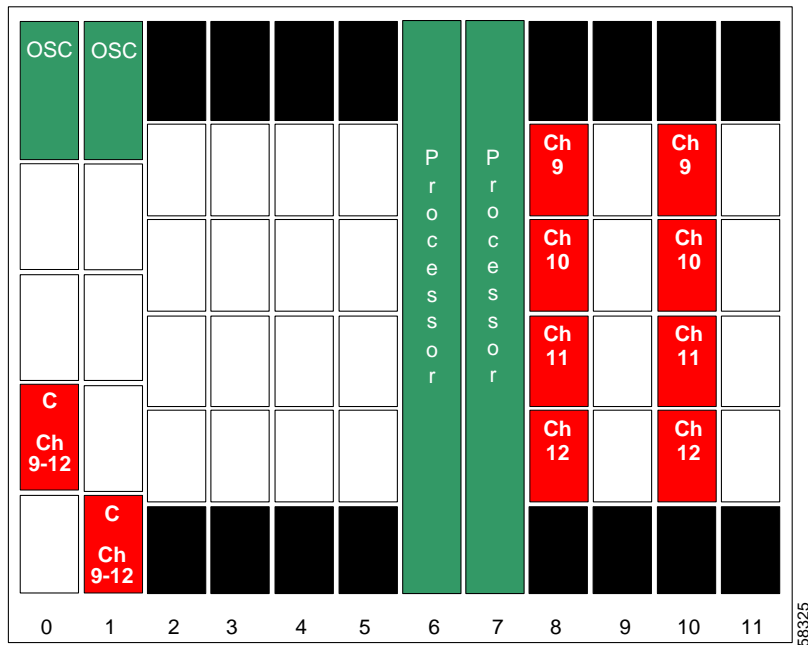
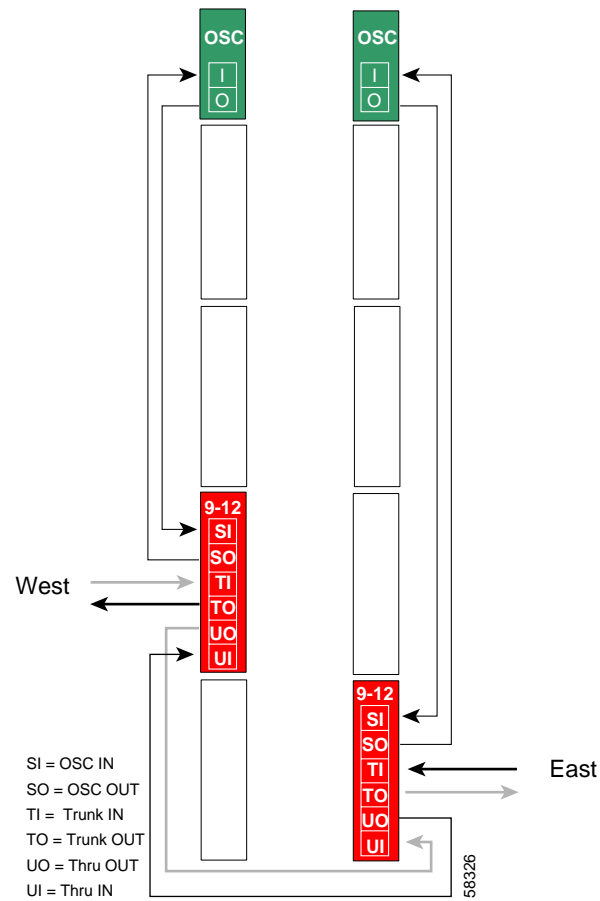


Figure 10-21 shows how the 4-channel mux/demux modules are cabled for node 4 in the line card protected hubbed ring shown in Figure 10-3 on page 10-4.

Figure 10-21 Add/Drop Mux/Demux Module Cabling with OSC for Node 4 in Line Card Protected Hubbed Ring



Patch Connections

```
Node4# configure terminal
Node4(config)# patch thru 0/2 thru 1/3
Node4(config)# patch wave 0 oscfilter 0/2
Node4(config)# patch wave 1 oscfilter 1/3

Node4(config)# patch wavepatch 8/0/0 filter 0/2/0
Node4(config)# patch wavepatch 8/1/0 filter 0/2/1
Node4(config)# patch wavepatch 8/2/0 filter 0/2/2
Node4(config)# patch wavepatch 8/3/0 filter 0/2/3

Node4(config)# patch wavepatch 10/0/0 filter 1/3/0
Node4(config)# patch wavepatch 10/1/0 filter 1/3/1
Node4(config)# patch wavepatch 10/2/0 filter 1/3/2
Node4(config)# patch wavepatch 10/3/0 filter 1/3/3
```

Transparent Interfaces in Slot 8

```
Node4 (config)# interface transparent 8/0/0
Node4 (config-if)# encapsulation gigabitethernet
Node4 (config-if)# monitor enable
Node4 (config-if)# exit
```

```
Node4 (config)# interface transparent 8/1/0
Node4 (config-if)# encapsulation gigabitethernet
Node4 (config-if)# monitor enable
Node4 (config-if)# exit
Node4 (config)# interface wave 8/1
Node4 (config-if)# laser frequency 193200
Node4 (config-if)# exit
```

```
Node4 (config)# interface transparent 8/2/0
Node4 (config-if)# encapsulation gigabitethernet
Node4 (config-if)# monitor enable
Node4 (config-if)# exit
```

```
Node4 (config)# interface transparent 8/3/0
Node4 (config-if)# encapsulation gigabitethernet
Node4 (config-if)# monitor enable
Node4 (config-if)# exit
Node4 (config)# interface wave 8/3
Node4 (config-if)# laser frequency 193400
Node4 (config-if)# exit
```

Transparent Interfaces in Slot 10

```
Node4 (config)# interface transparent 10/0/0
Node4 (config-if)# encapsulation gigabitethernet
Node4 (config-if)# monitor enable
Node4 (config-if)# exit
```

```
Node4 (config)# interface transparent 10/1/0
Node4 (config-if)# encapsulation gigabitethernet
Node4 (config-if)# monitor enable
Node4 (config-if)# exit
Node4 (config)# interface wave 10/1
Node4 (config-if)# laser frequency 193200
Node4 (config-if)# exit
```

```
Node4 (config)# interface transparent 10/2/0
Node4 (config-if)# encapsulation gigabitethernet
Node4 (config-if)# monitor enable
Node4 (config-if)# exit
```

```
Node4 (config)# interface transparent 10/3/0
Node4 (config-if)# encapsulation gigabitethernet
Node4 (config-if)# monitor enable
Node4 (config-if)# exit
Node4 (config)# interface wave 10/3
Node4 (config-if)# laser frequency 193400
Node4 (config-if)# exit
```

OSC Interfaces

```
Node4 (config)# interface wave 0
Node4 (config-if)# no shutdown
```

```
Node4(config-if)# exit

Node4(config)# interface wave 1
Node4(config-if)# no shutdown
Node4(config-if)# exit
```

APS

Use the following for configuring y-cable protection.

```
Node4(config)# redundancy
Node4(config-red)# associate group channel9
Node4(config-red-aps)# aps working transparent 10/0/0
Node4(config-red-aps)# aps protection transparent 8/0/0
Node4(config-red-aps)# aps y-cable
Node4(config-red-aps)# aps revertive
Node4(config-red-aps)# aps enable
Node4(config-red-aps)# exit
Node4(config-red)# associate group channel10
Node4(config-red-aps)# aps working transparent 10/1/0
Node4(config-red-aps)# aps protection transparent 8/1/0
Node4(config-red-aps)# aps y-cable
Node4(config-red-aps)# aps revertive
Node4(config-red-aps)# aps enable
Node4(config-red-aps)# exit
Node4(config-red)# associate group channel11
Node4(config-red-aps)# aps working transparent 10/2/0
Node4(config-red-aps)# aps protection transparent 8/2/0
Node4(config-red-aps)# aps y-cable
Node4(config-red-aps)# aps revertive
Node4(config-red-aps)# aps enable
Node4(config-red-aps)# exit
Node4(config-red)# associate group channel12
Node4(config-red-aps)# aps working transparent 10/3/0
Node4(config-red-aps)# aps protection transparent 8/3/0
Node4(config-red-aps)# aps y-cable
Node4(config-red-aps)# aps revertive
Node4(config-red-aps)# aps enable
Node4(config-red-aps)# end

Node4# copy system:running-config nvram:startup-config
```

Node 5

Figure 10-22 shows the shelf configuration for node 5 in the line card protected hubbed ring shown in Figure 10-3 on page 10-4. Slot 9 uses a nonsplitter line card motherboard that cross connects the signal to the add/drop mux/demux module in the east mux/demux slot 1; slot 11 uses a nonsplitter line card motherboard that cross connects the signal cross connect to the add/drop mux/demux module in the west mux/demux slot 0.

Figure 10-22 Shelf Configuration for Node 5 in Line Card Protected Hubbed Ring

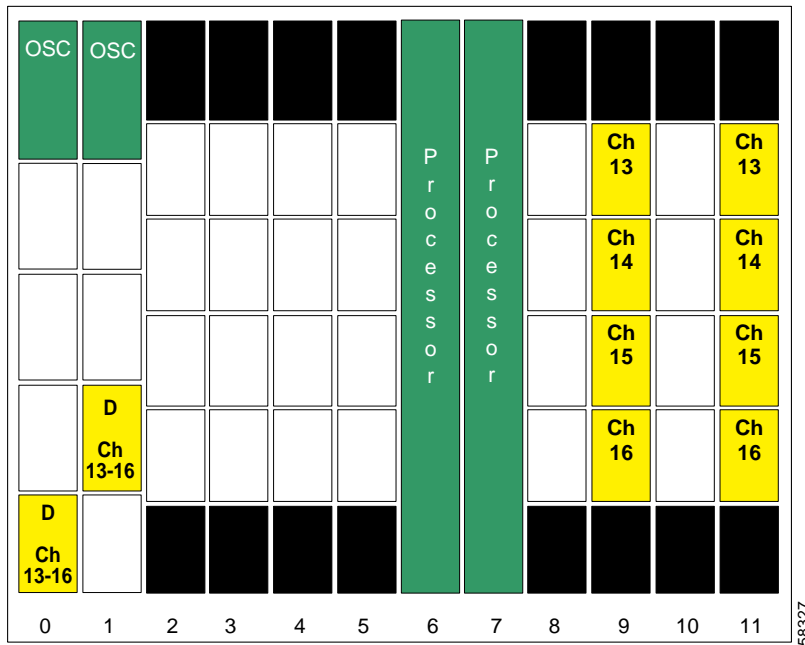
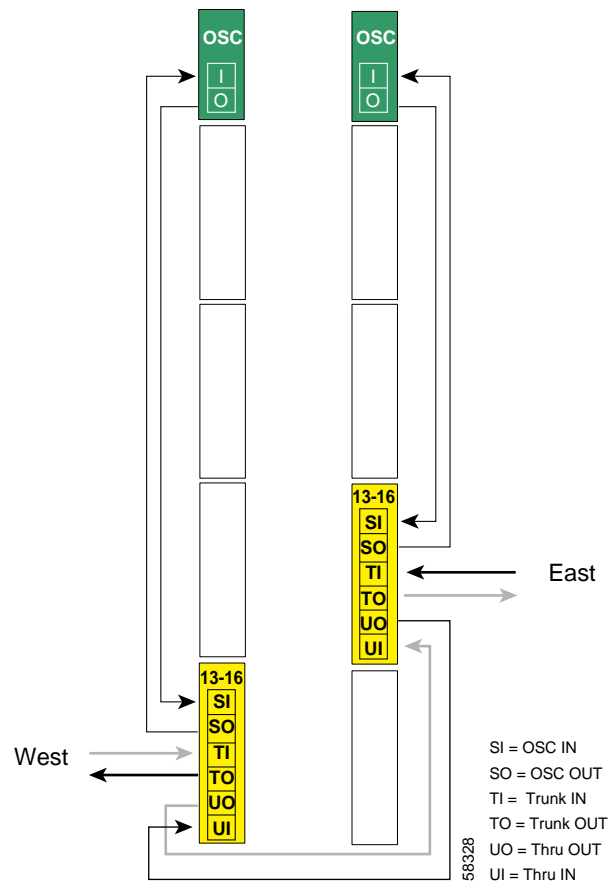


Figure 10-23 shows how the 4-channel mux/demux modules are cabled for node 5 in the line card protected hubbed ring shown in Figure 10-3 on page 10-4.

Figure 10-23 Add/Drop Mux/Demux Module Cabling with OSC for Node 5 in Line Card Protected Hubbed Ring



Patch Connections

```

Node5# configure terminal
Node5(config)# patch thru 0/3 thru 1/2
Node5(config)# patch wave 0 oscfilter 0/3
Node5(config)# patch wave 1 oscfilter 1/2

Node5(config)# patch wavepatch 9/0/0 filter 0/3/0
Node5(config)# patch wavepatch 9/1/0 filter 0/3/1
Node5(config)# patch wavepatch 9/2/0 filter 0/3/2
Node5(config)# patch wavepatch 9/3/0 filter 0/3/3

Node5(config)# patch wavepatch 11/0/0 filter 1/2/0
Node5(config)# patch wavepatch 11/1/0 filter 1/2/1
Node5(config)# patch wavepatch 11/2/0 filter 1/2/2
Node5(config)# patch wavepatch 11/3/0 filter 1/2/3
  
```

Transparent Interfaces in Slot 9

```
Node5 (config)# interface transparent 9/0/0
Node5 (config-if)# encapsulation gigabitethernet
Node5 (config-if)# monitor enable
Node5 (config-if)# exit
```

```
Node5 (config)# interface transparent 9/1/0
Node5 (config-if)# encapsulation gigabitethernet
Node5 (config-if)# monitor enable
Node5 (config-if)# exit
Node5 (config)# interface wave 9/1
Node5 (config-if)# laser frequency 1953700
Node5 (config-if)# exit
```

```
Node5 (config)# interface transparent 9/2/0
Node5 (config-if)# encapsulation gigabitethernet
Node5 (config-if)# monitor enable
Node5 (config-if)# exit
```

```
Node5 (config)# interface transparent 9/3/0
Node5 (config-if)# encapsulation gigabitethernet
Node5 (config-if)# monitor enable
Node5 (config-if)# exit
Node5 (config)# interface wave 9/3
Node5 (config-if)# laser frequency 193900
Node5 (config-if)# exit
```

Transparent Interfaces in Slot 11

```
Node5 (config)# interface transparent 11/0/0
Node5 (config-if)# encapsulation gigabitethernet
Node5 (config-if)# monitor enable
Node5 (config-if)# exit
```

```
Node5 (config)# interface transparent 11/1/0
Node5 (config-if)# encapsulation gigabitethernet
Node5 (config-if)# monitor enable
Node5 (config-if)# exit
Node5 (config)# interface wave 11/1
Node5 (config-if)# laser frequency 1953700
Node5 (config-if)# exit
```

```
Node5 (config)# interface transparent 11/2/0
Node5 (config-if)# encapsulation gigabitethernet
Node5 (config-if)# monitor enable
Node5 (config-if)# exit
```

```
Node5 (config)# interface transparent 11/3/0
Node5 (config-if)# encapsulation gigabitethernet
Node5 (config-if)# monitor enable
Node5 (config-if)# exit
Node5 (config)# interface wave 11/3
Node5 (config-if)# laser frequency 193900
Node5 (config-if)# exit
```

OSC Interfaces

```
Node5 (config)# interface wave 0
Node5 (config-if)# no shutdown
```

```
Node5(config-if)# exit

Node5(config)# interface wave 1
Node5(config-if)# no shutdown
Node5(config-if)# exit
```

APS

Use the following for configuring y-cable protection.

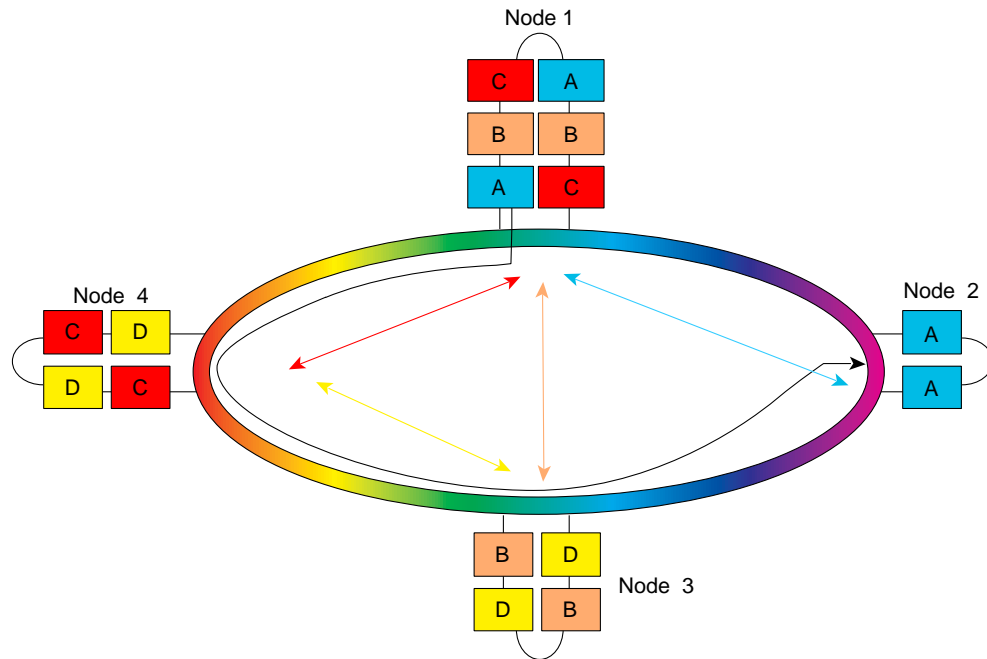
```
Node5(config)# redundancy
Node5(config-red)# associate group channel13
Node5(config-red-aps)# aps working transparent 9/0/0
Node5(config-red-aps)# aps protection transparent 11/0/0
Node5(config-red-aps)# aps y-cable
Node5(config-red-aps)# aps revertive
Node5(config-red-aps)# aps enable
Node5(config-red-aps)# exit
Node5(config-red)# associate group channel14
Node5(config-red-aps)# aps working transparent 9/1/0
Node5(config-red-aps)# aps protection transparent 11/1/0
Node5(config-red-aps)# aps y-cable
Node5(config-red-aps)# aps revertive
Node5(config-red-aps)# aps enable
Node5(config-red-aps)# exit
Node5(config-red)# associate group channel15
Node5(config-red-aps)# aps working transparent 9/2/0
Node5(config-red-aps)# aps protection transparent 11/2/0
Node5(config-red-aps)# aps y-cable
Node5(config-red-aps)# aps revertive
Node5(config-red-aps)# aps enable
Node5(config-red-aps)# exit
Node5(config-red)# associate group channel16
Node5(config-red-aps)# aps working transparent 9/3/0
Node5(config-red-aps)# aps protection transparent 11/3/0
Node5(config-red-aps)# aps y-cable
Node5(config-red-aps)# aps revertive
Node5(config-red-aps)# aps enable
Node5(config-red-aps)# end

Node5# copy system:running-config nvram:startup-config
```

Configuring a Meshed Ring with Splitter Protection and OSC

Figure 10-24 shows an example topology of a four-node meshed ring with splitter protection and OSC support. Node 1 supports bands A, B, and C (channels 1 through 12). Node 2 adds and drops band A, node 3 adds and drops band B and band D, and node 4 adds and drops band C and band D. The transponders carry Gigabit Ethernet traffic.

Figure 10-24 Channel Plan for Meshed Ring



58490

Node 1

Figure 10-25 shows the shelf configuration for node 1 in the splitter protected meshed ring shown in Figure 10-24 on page 10-46. Splitter line card motherboards are used to cross connect the signal to the add/drop mux/demux modules in both west and east mux/demux slots 0 and 1.

Figure 10-25 Shelf Configuration for Node 1 in Splitter Protected Meshed Ring

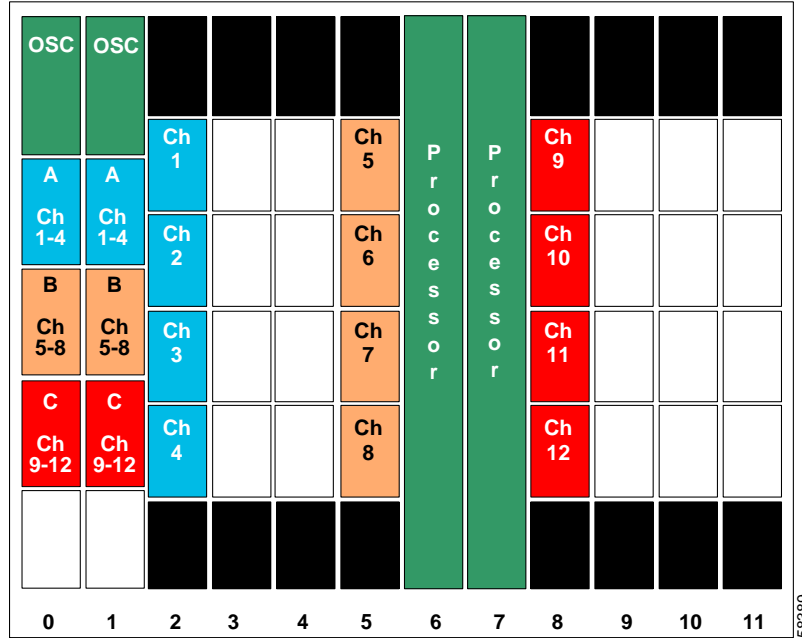
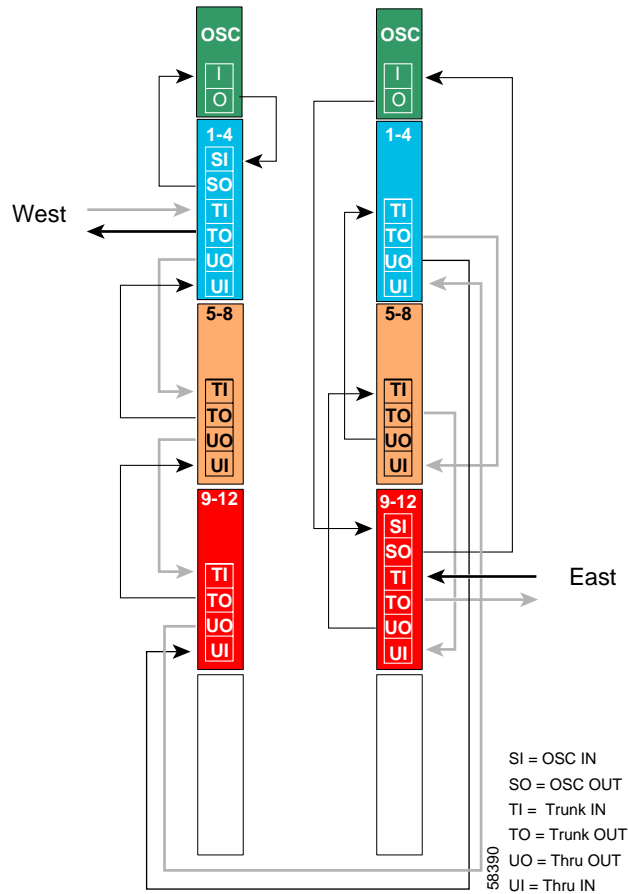


Figure 10-26 shows how the 4-channel mux/demux modules are cabled for node 1 in the splitter protected meshed ring shown in Figure 10-24 on page 10-46.

Figure 10-26 Add/Drop Mux/Demux Module Cabling with OSC for Node 1 in Splitter Protected Meshed Ring



Patch Connections

```

Node1# configure terminal
Node1(config)# patch thru 0/0 wdm 0/1
Node1(config)# patch thru 0/1 wdm 0/2
Node1(config)# patch thru 0/2 thru 1/0
Node1(config)# patch wdm 1/0 thru 1/1
Node1(config)# patch wdm 1/1 thru 1/2
Node1(config)# patch wave 0 oscfilter 0/0
Node1(config)# patch wave 1 oscfilter 1/2

Node1(config)# patch wavepatch 2/0/0 filter 0/0/0
Node1(config)# patch wavepatch 2/1/0 filter 0/0/1
Node1(config)# patch wavepatch 2/2/0 filter 0/0/2
Node1(config)# patch wavepatch 2/3/0 filter 0/0/3
Node1(config)# patch wavepatch 2/0/1 filter 1/0/0
Node1(config)# patch wavepatch 2/1/1 filter 1/0/1
Node1(config)# patch wavepatch 2/2/1 filter 1/0/2
Node1(config)# patch wavepatch 2/3/1 filter 1/0/3
  
```

```
Node1(config)# patch wavepatch 5/0/0 filter 0/1/0
Node1(config)# patch wavepatch 5/1/0 filter 0/1/1
Node1(config)# patch wavepatch 5/2/0 filter 0/1/2
Node1(config)# patch wavepatch 5/3/0 filter 0/1/3
Node1(config)# patch wavepatch 5/0/1 filter 1/1/0
Node1(config)# patch wavepatch 5/1/1 filter 1/1/1
Node1(config)# patch wavepatch 5/2/1 filter 1/1/2
Node1(config)# patch wavepatch 5/3/1 filter 1/1/3

Node1(config)# patch wavepatch 8/0/0 filter 0/2/0
Node1(config)# patch wavepatch 8/1/0 filter 0/2/1
Node1(config)# patch wavepatch 8/2/0 filter 0/2/2
Node1(config)# patch wavepatch 8/3/0 filter 0/2/3
Node1(config)# patch wavepatch 8/0/1 filter 1/2/0
Node1(config)# patch wavepatch 8/1/1 filter 1/2/1
Node1(config)# patch wavepatch 8/2/1 filter 1/2/2
Node1(config)# patch wavepatch 8/3/1 filter 1/2/3
```

Transparent Interfaces in Slot 2

```
Node1(config)# interface transparent 2/0/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 2/1/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 2/1
Node1(config-if)# laser frequency 192200
Node1(config-if)# exit

Node1(config)# interface transparent 2/2/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 2/3/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 2/3
Node1(config-if)# laser frequency 192400
Node1(config-if)# exit
```

Transparent Interfaces in Slot 5

```
Node1(config)# interface transparent 5/0/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 5/1/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 5/1
```

```

Node1(config-if)# laser frequency 192700
Node1(config-if)# exit

Node1(config)# interface transparent 5/2/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 5/3/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 5/3
Node1(config-if)# laser frequency 192900
Node1(config-if)# exit

```

Transparent Interfaces in Slot 8

```

Node1(config)# interface transparent 8/0/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 8/1/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 8/1
Node1(config-if)# laser frequency 193200
Node1(config-if)# exit

Node1(config)# interface transparent 8/2/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 8/3/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 8/3
Node1(config-if)# laser frequency 193400
Node1(config-if)# exit

```

OSC Interfaces

```

Node1(config)# interface wave 0
Node1(config-if)# no shutdown
Node1(config-if)# exit

Node1(config)# interface wave 1
Node1(config-if)# no shutdown
Node1(config-if)# exit

```

APS

```

Node1(config)# redundancy
Node1(config-red)# associate group channel1

```

```
Node1(config-red-aps)# aps working wavepatch 2/0/1
Node1(config-red-aps)# aps protection wavepatch 2/0/0
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel2
Node1(config-red-aps)# aps working wavepatch 2/1/1
Node1(config-red-aps)# aps protection wavepatch 2/1/0
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel3
Node1(config-red-aps)# aps working wavepatch 2/2/1
Node1(config-red-aps)# aps protection wavepatch 2/2/0
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel4
Node1(config-red-aps)# aps working wavepatch 2/3/1
Node1(config-red-aps)# aps protection wavepatch 2/3/0
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit

Node1(config-red)# associate group channel5
Node1(config-red-aps)# aps working wavepatch 5/0/1
Node1(config-red-aps)# aps protection wavepatch 5/0/0
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel6
Node1(config-red-aps)# aps working wavepatch 5/1/1
Node1(config-red-aps)# aps protection wavepatch 5/1/0
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel7
Node1(config-red-aps)# aps working wavepatch 5/2/1
Node1(config-red-aps)# aps protection wavepatch 5/2/0
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel8
Node1(config-red-aps)# aps working wavepatch 5/3/1
Node1(config-red-aps)# aps protection wavepatch 5/3/0
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit

Node1(config-red)# associate group channel9
Node1(config-red-aps)# aps working wavepatch 8/0/0
Node1(config-red-aps)# aps protection wavepatch 8/0/1
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel10
Node1(config-red-aps)# aps working wavepatch 8/1/0
Node1(config-red-aps)# aps protection wavepatch 8/1/1
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel11
Node1(config-red-aps)# aps working wavepatch 8/2/0
Node1(config-red-aps)# aps protection wavepatch 8/2/1
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel12
Node1(config-red-aps)# aps working wavepatch 8/3/0
Node1(config-red-aps)# aps protection wavepatch 8/3/1
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# end

Node1# copy system:running-config nvram:startup-config
```

Node 2

Figure 10-27 shows the shelf configuration for node 2 in the splitter protected meshed ring shown in Figure 10-24 on page 10-46. Slot 2 uses the splitter line card motherboard, which cross connects the signal to the add/drop mux/demux modules in both west and east mux/demux slots 0 and 1.

Figure 10-27 Shelf Configuration for Node 2 in Splitter Protected Meshed Ring

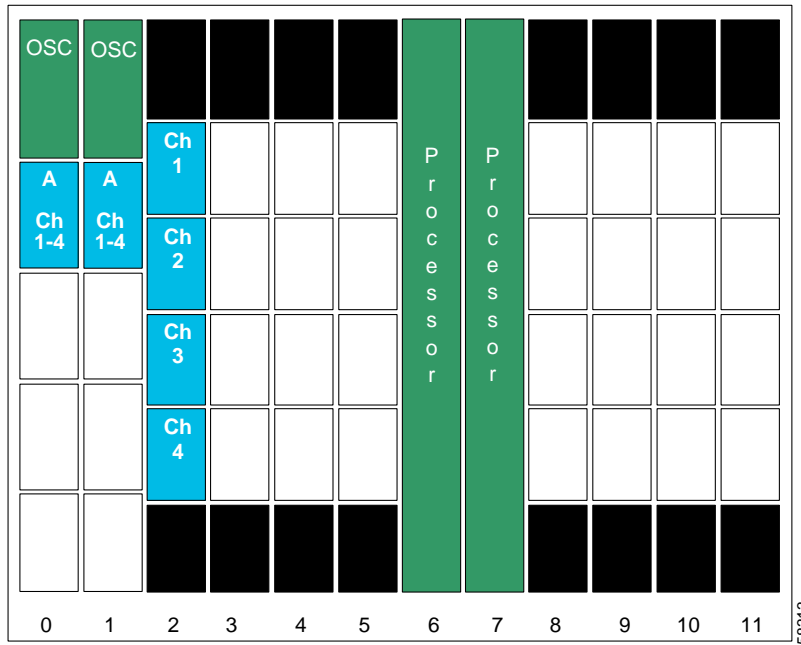
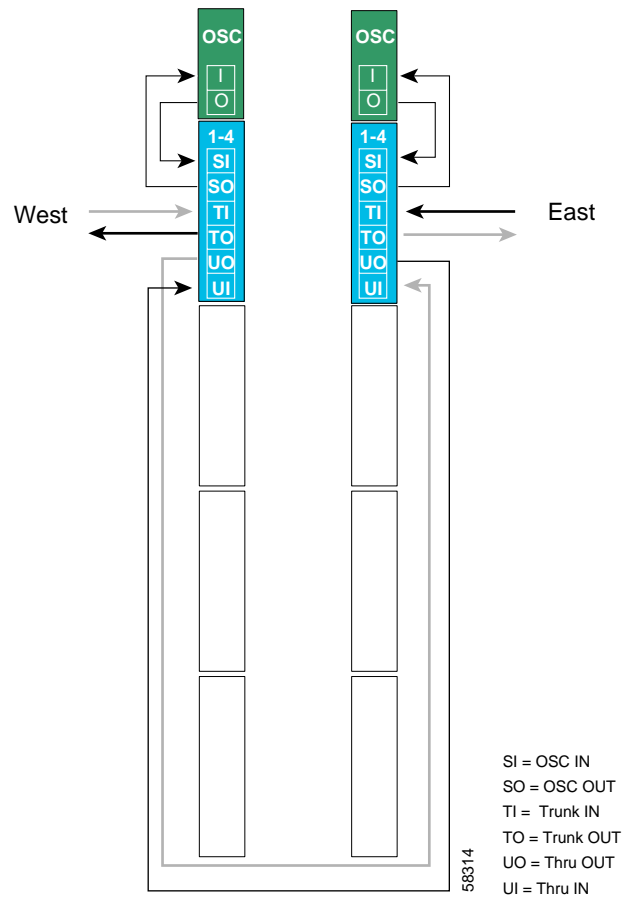


Figure 10-28 shows how the 4-channel mux/demux modules are cabled for node 2 in the splitter protected meshed ring shown in Figure 10-24 on page 10-46.

Figure 10-28 Add/Drop Mux/Demux Module Cabling with OSC for Node 2 in Splitter Protected Meshed Ring



Patch Connections

```

Node2# configure terminal
Node2(config)# patch thru 0/0 thru 1/0
Node2(config)# patch wave 0 oscfilter 0/0
Node2(config)# patch wave 1 oscfilter 1/0

Node2(config)# patch wavepatch 2/0/0 filter 0/0/0
Node2(config)# patch wavepatch 2/1/0 filter 0/0/1
Node2(config)# patch wavepatch 2/2/0 filter 0/0/2
Node2(config)# patch wavepatch 2/3/0 filter 0/0/3
Node2(config)# patch wavepatch 2/0/1 filter 1/0/0
Node2(config)# patch wavepatch 2/1/1 filter 1/0/1
Node2(config)# patch wavepatch 2/2/1 filter 1/0/2
Node2(config)# patch wavepatch 2/3/1 filter 1/0/3
  
```

Transparent Interfaces in Slot 2

```
Node2(config)# interface transparent 2/0/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 2/1/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
Node2(config)# interface wave 2/1
Node2(config-if)# laser frequency 192200
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 2/2/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 2/3/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
Node2(config)# interface wave 2/3
Node2(config-if)# laser frequency 192400
Node2(config-if)# exit
```

OSC Interfaces

```
Node2(config)# interface wave 0
Node2(config-if)# no shutdown
Node2(config-if)# exit
```

```
Node2(config)# interface wave 1
Node2(config-if)# no shutdown
Node2(config-if)# exit
```

APS

```
Node2(config)# redundancy
Node2(config-red)# associate group channel1
Node2(config-red-aps)# aps working wavepatch 2/0/0
Node2(config-red-aps)# aps protection wavepatch 2/0/1
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# exit
Node2(config-red)# associate group channel2
Node2(config-red-aps)# aps working wavepatch 2/1/0
Node2(config-red-aps)# aps protection wavepatch 2/1/1
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# exit
Node2(config-red)# associate group channel3
Node2(config-red-aps)# aps working wavepatch 2/2/0
Node2(config-red-aps)# aps protection wavepatch 2/2/1
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# exit
Node2(config-red)# associate group channel4
Node2(config-red-aps)# aps working wavepatch 2/3/0
Node2(config-red-aps)# aps protection wavepatch 2/3/1
```



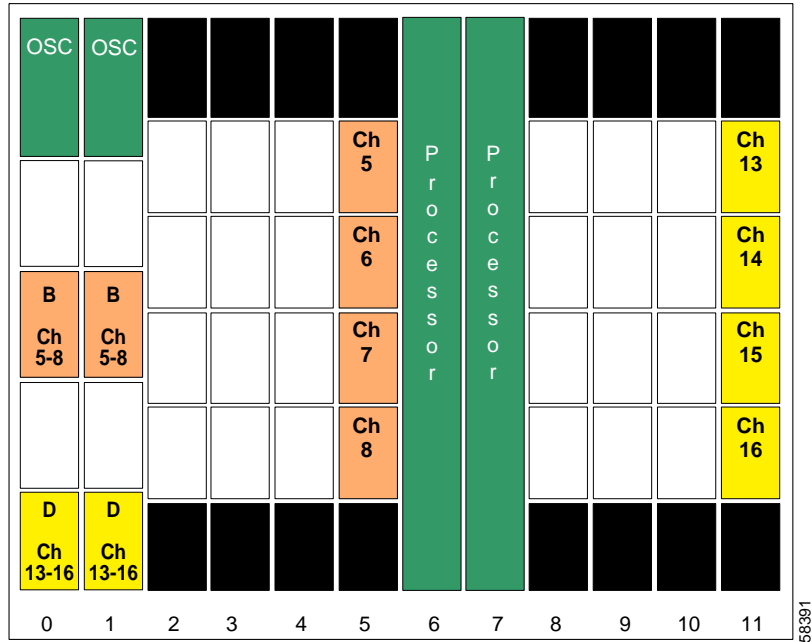
```
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# end

Node2# copy system:running-config nvram:startup-config
```

Node 3

Figure 10-29 shows the shelf configuration for node 3 in the splitter protected meshed ring shown in Figure 10-24 on page 10-46. Slots 5 and 11 use splitter line card motherboards, which cross connect the signal to the add/drop mux/demux modules in both west and east mux/demux slots 0 and 1.

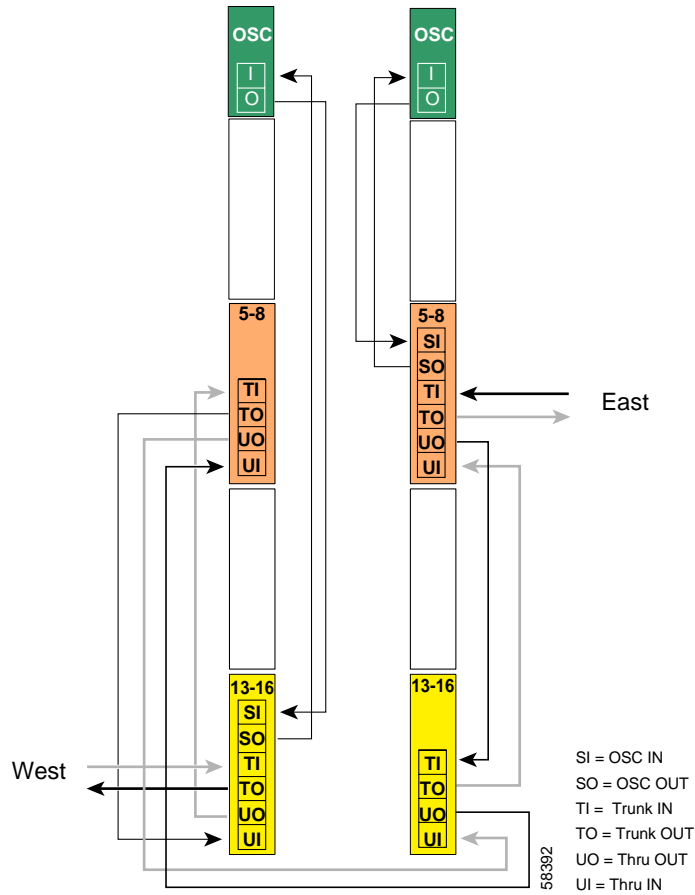
Figure 10-29 Shelf Configuration for Node 3 in Splitter Protected Meshed Ring



58391

Figure 10-30 shows how the 4-channel mux/demux modules are cabled for node 3 in the splitter protected meshed ring shown in Figure 10-24 on page 10-46.

Figure 10-30 Add/Drop Mux/Demux Module Cabling with OSC for Node 3 in Splitter Protected Meshed Ring



Patch Connections

```

Node3# configure terminal
Node3(config)# patch wdm 0/1 thru 0/3
Node3(config)# patch thru 0/1 thru 1/3
Node3(config)# patch wdm 1/3 thru 1/1
Node3(config)# patch wave 0 oscfilter 0/3
Node3(config)# patch wave 1 oscfilter 1/1

Node3(config)# patch wavepatch 5/0/0 filter 0/1/0
Node3(config)# patch wavepatch 5/1/0 filter 0/1/1
Node3(config)# patch wavepatch 5/2/0 filter 0/1/2
Node3(config)# patch wavepatch 5/3/0 filter 0/1/3
Node3(config)# patch wavepatch 5/0/1 filter 1/1/0
Node3(config)# patch wavepatch 5/1/1 filter 1/1/1
Node3(config)# patch wavepatch 5/2/1 filter 1/1/2
Node3(config)# patch wavepatch 5/3/1 filter 1/1/3

Node3(config)# patch wavepatch 11/0/0 filter 0/3/0

```

```
Node3(config)# patch wavepatch 11/1/0 filter 0/3/1
Node3(config)# patch wavepatch 11/2/0 filter 0/3/2
Node3(config)# patch wavepatch 11/3/0 filter 0/3/3
Node3(config)# patch wavepatch 11/0/1 filter 1/3/0
Node3(config)# patch wavepatch 11/1/1 filter 1/3/1
Node3(config)# patch wavepatch 11/2/1 filter 1/3/2
Node3(config)# patch wavepatch 11/3/1 filter 1/3/3
```

Transparent Interfaces in Slot 5

```
Node3(config)# interface transparent 5/0/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
```

```
Node3(config)# interface transparent 5/1/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
Node3(config)# interface wave 5/1
Node3(config-if)# laser frequency 192700
Node3(config-if)# exit
```

```
Node3(config)# interface transparent 5/2/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
```

```
Node3(config)# interface transparent 5/3/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
Node3(config)# interface wave 5/3
Node3(config-if)# laser frequency 192900
Node3(config-if)# exit
```

Transparent Interfaces in Slot 11

```
Node3(config)# interface transparent 11/0/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
```

```
Node3(config)# interface transparent 11/1/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
Node3(config)# interface wave 11/1
Node3(config-if)# laser frequency 1953700
Node3(config-if)# exit
```

```
Node3(config)# interface transparent 11/2/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
```

```
Node3(config)# interface transparent 11/3/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
```

```

Node3(config-if)# exit
Node3(config)# interface wave 11/3
Node3(config-if)# laser frequency 193900
Node3(config-if)# exit

```

OSC Interfaces

```

Node3(config)# interface wave 0
Node3(config-if)# no shutdown
Node3(config-if)# exit

```

```

Node3(config)# interface wave 1
Node3(config-if)# no shutdown
Node3(config-if)# exit

```

APS

```

Node3(config)# redundancy
Node3(config-red)# associate group channel5
Node3(config-red-aps)# aps working wavepatch 5/0/0
Node3(config-red-aps)# aps protection wavepatch 5/0/1
Node3(config-red-aps)# aps enable
Node3(config-red-aps)# exit
Node3(config-red)# associate group channel6
Node3(config-red-aps)# aps working wavepatch 5/1/0
Node3(config-red-aps)# aps protection wavepatch 5/1/1
Node3(config-red-aps)# aps enable
Node3(config-red-aps)# exit
Node3(config-red)# associate group channel7
Node3(config-red-aps)# aps working wavepatch 5/2/0
Node3(config-red-aps)# aps protection wavepatch 5/2/1
Node3(config-red-aps)# aps enable
Node3(config-red-aps)# exit
Node3(config-red)# associate group channel8
Node3(config-red-aps)# aps working wavepatch 5/3/0
Node3(config-red-aps)# aps protection wavepatch 5/3/1
Node3(config-red-aps)# aps enable
Node3(config-red-aps)# exit

Node3(config-red)# associate group channel13
Node3(config-red-aps)# aps working wavepatch 11/0/1
Node3(config-red-aps)# aps protection wavepatch 11/0/0
Node3(config-red-aps)# aps enable
Node3(config-red-aps)# exit
Node3(config-red)# associate group channel14
Node3(config-red-aps)# aps working wavepatch 11/1/1
Node3(config-red-aps)# aps protection wavepatch 11/1/0
Node3(config-red-aps)# aps enable
Node3(config-red-aps)# exit
Node3(config-red)# associate group channel15
Node3(config-red-aps)# aps working wavepatch 11/2/1
Node3(config-red-aps)# aps protection wavepatch 11/2/0
Node3(config-red-aps)# aps enable
Node3(config-red-aps)# exit
Node3(config-red)# associate group channel16
Node3(config-red-aps)# aps working wavepatch 11/3/1
Node3(config-red-aps)# aps protection wavepatch 11/3/0
Node3(config-red-aps)# aps enable
Node3(config-red-aps)# end

```

```

Node3# copy system:running-config nvram:startup-config

```

Node 4

Figure 10-31 shows the shelf configuration for node 4 in the splitter protected meshed ring shown in Figure 10-24 on page 10-46. Slots 8 and 11 use the splitter line card motherboards, which cross connect the signal to the add/drop mux/demux modules in both the west and east mux/demux slots 0 and 1.

Figure 10-31 Module Installation Configuration for Node 4

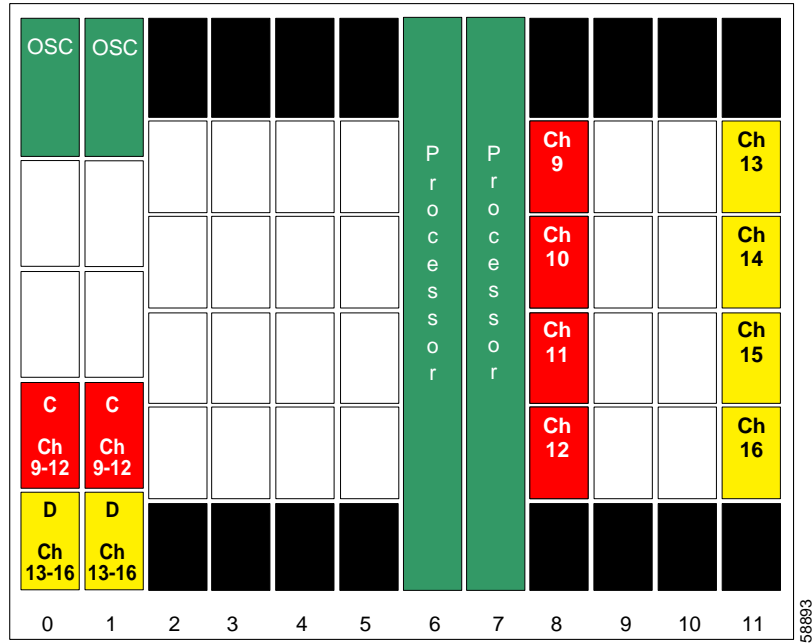
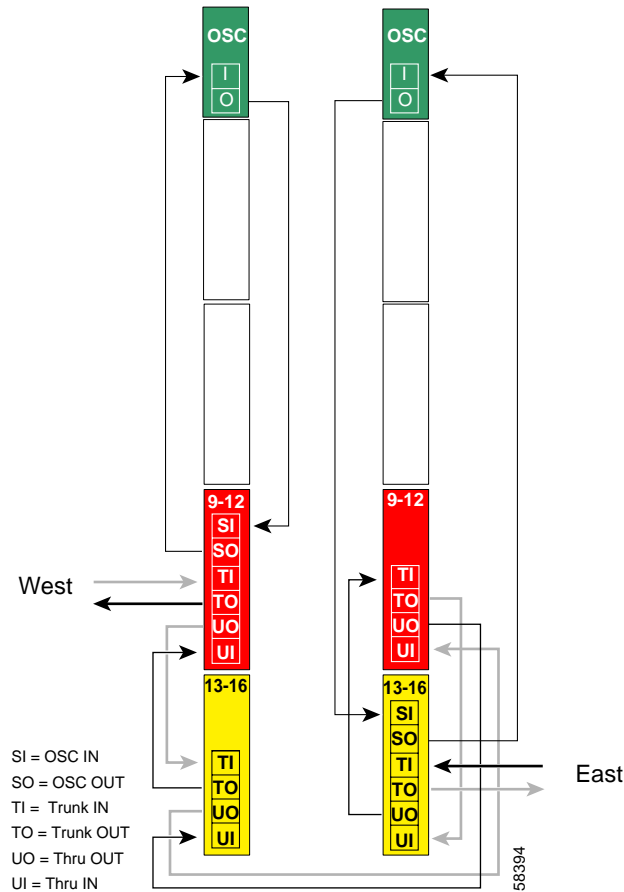


Figure 10-32 shows how the 4-channel mux/demux modules are cabled for node 4 in the splitter protected meshed ring shown in Figure 10-24 on page 10-46.

Figure 10-32 Add/Drop Mux/Demux Module Cabling with OSC for Node 4 in Splitter Protected Meshed Ring



Patch Connections

```

Node4# configure terminal
Node4 (config)# patch thru 0/2 wdm 0/3
Node4 (config)# patch thru 0/3 thru 1/2
Node4 (config)# patch wdm 1/2 thru 1/3
Node4 (config)# patch wave 0 oscfilter 0/2
Node4 (config)# patch wave 1 oscfilter 1/3

Node4 (config)# patch wavepatch 8/0/0 filter 0/2/0
Node4 (config)# patch wavepatch 8/1/0 filter 0/2/1
Node4 (config)# patch wavepatch 8/2/0 filter 0/2/2
Node4 (config)# patch wavepatch 8/3/0 filter 0/2/3
Node4 (config)# patch wavepatch 8/0/1 filter 1/2/0
Node4 (config)# patch wavepatch 8/1/1 filter 1/2/1
Node4 (config)# patch wavepatch 8/2/1 filter 1/2/2
Node4 (config)# patch wavepatch 8/3/1 filter 1/2/3

Node4 (config)# patch wavepatch 11/0/0 filter 0/3/0
  
```

```
Node4(config)# patch wavepatch 11/1/0 filter 0/3/1
Node4(config)# patch wavepatch 11/2/0 filter 0/3/2
Node4(config)# patch wavepatch 11/3/0 filter 0/3/3
Node4(config)# patch wavepatch 11/0/1 filter 1/3/0
Node4(config)# patch wavepatch 11/1/1 filter 1/3/1
Node4(config)# patch wavepatch 11/2/1 filter 1/3/2
Node4(config)# patch wavepatch 11/3/1 filter 1/3/3
```

Transparent Interfaces in Slot 8

```
Node4(config)# interface transparent 8/0/0
Node4(config-if)# encapsulation gigabitethernet
Node4(config-if)# monitor enable
Node4(config-if)# exit
```

```
Node4(config)# interface transparent 8/1/0
Node4(config-if)# encapsulation gigabitethernet
Node4(config-if)# monitor enable
Node4(config-if)# exit
Node4(config)# interface wave 8/1
Node4(config-if)# laser frequency 193200
Node4(config-if)# exit
```

```
Node4(config)# interface transparent 8/2/0
Node4(config-if)# encapsulation gigabitethernet
Node4(config-if)# monitor enable
Node4(config-if)# exit
```

```
Node4(config)# interface transparent 8/3/0
Node4(config-if)# encapsulation gigabitethernet
Node4(config-if)# monitor enable
Node4(config-if)# exit
Node4(config)# interface wave 8/3
Node4(config-if)# laser frequency 193400
Node4(config-if)# exit
```

Transparent Interfaces in Slot 11

```
Node4(config)# interface transparent 11/0/0
Node4(config-if)# encapsulation gigabitethernet
Node4(config-if)# monitor enable
Node4(config-if)# exit
```

```
Node4(config)# interface transparent 11/1/0
Node4(config-if)# encapsulation gigabitethernet
Node4(config-if)# monitor enable
Node4(config-if)# exit
Node4(config)# interface wave 11/1
Node4(config-if)# laser frequency 1953700
Node4(config-if)# exit
```

```
Node4(config)# interface transparent 11/2/0
Node4(config-if)# encapsulation gigabitethernet
Node4(config-if)# monitor enable
Node4(config-if)# exit
```

```
Node4(config)# interface transparent 11/3/0
Node4(config-if)# encapsulation gigabitethernet
Node4(config-if)# monitor enable
```

```

Node4 (config-if)# exit
Node4 (config)# interface wave 11/3
Node4 (config-if)# laser frequency 193900
Node4 (config-if)# exit

```

OSC Interfaces

```

Node4 (config)# interface wave 0
Node4 (config-if)# no shutdown
Node4 (config-if)# exit

```

```

Node4 (config)# interface wave 1
Node4 (config-if)# no shutdown
Node4 (config-if)# exit

```

APS

```

Node4 (config)# redundancy
Node4 (config-red)# associate group channel9
Node4 (config-red-aps)# aps working wavepatch 8/0/1
Node4 (config-red-aps)# aps protection wavepatch 8/0/0
Node4 (config-red-aps)# aps enable
Node4 (config-red-aps)# exit
Node4 (config-red)# associate group channel10
Node4 (config-red-aps)# aps working wavepatch 8/1/1
Node4 (config-red-aps)# aps protection wavepatch 8/1/0
Node4 (config-red-aps)# aps enable
Node4 (config-red-aps)# exit
Node4 (config-red)# associate group channel11
Node4 (config-red-aps)# aps working wavepatch 8/2/1
Node4 (config-red-aps)# aps protection wavepatch 8/2/0
Node4 (config-red-aps)# aps enable
Node4 (config-red-aps)# exit
Node4 (config-red)# associate group channel12
Node4 (config-red-aps)# aps working wavepatch 8/3/1
Node4 (config-red-aps)# aps protection wavepatch 8/3/0
Node4 (config-red-aps)# aps enable
Node4 (config-red-aps)# exit

Node4 (config-red)# associate group channel13
Node4 (config-red-aps)# aps working wavepatch 11/0/0
Node4 (config-red-aps)# aps protection wavepatch 11/0/1
Node4 (config-red-aps)# aps enable
Node4 (config-red-aps)# exit
Node4 (config-red)# associate group channel14
Node4 (config-red-aps)# aps working wavepatch 11/1/0
Node4 (config-red-aps)# aps protection wavepatch 11/1/1
Node4 (config-red-aps)# aps enable
Node4 (config-red-aps)# exit
Node4 (config-red)# associate group channel15
Node4 (config-red-aps)# aps working wavepatch 11/2/0
Node4 (config-red-aps)# aps protection wavepatch 11/2/1
Node4 (config-red-aps)# aps enable
Node4 (config-red-aps)# exit
Node4 (config-red)# associate group channel16
Node4 (config-red-aps)# aps working wavepatch 11/3/0
Node4 (config-red-aps)# aps protection wavepatch 11/3/1
Node4 (config-red-aps)# aps enable
Node4 (config-red-aps)# end

```

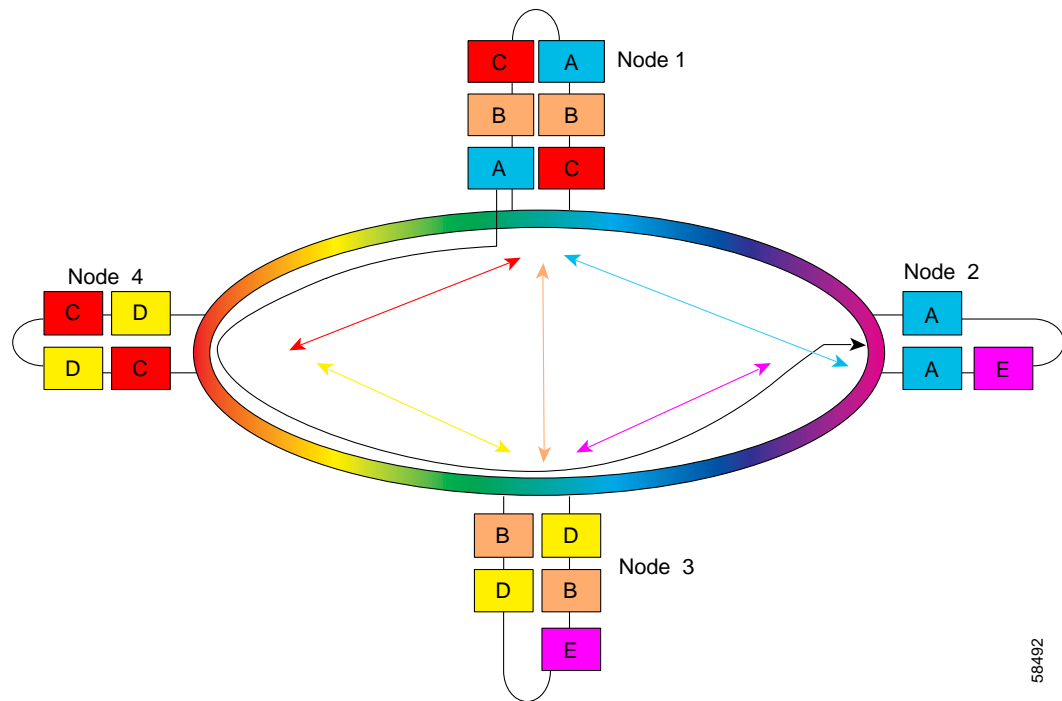


```
Node4# copy system:running-config nvram:startup-config
```

Configuring a Splitter Protected Meshed Ring with Unprotected Channels and OSC

Figure 10-33 shows an example topology of a four-node meshed ring with splitter protection and OSC support. Node 1 supports bands A, B, and C (channels 1-12). Node 2 adds and drops band A (channels 1-4) and unprotected band E (channels 17-20). Node 3 adds and drops band B (channels 5-8), band D (channels 13-16), and unprotected band E (channels 17-20). Node 4 adds and drops band C (channels 9-12) and band D (channels 13-16). The transponders carry Gigabit Ethernet traffic.

Figure 10-33 Overview of Meshed Ring Topology with Splitter Protection



58492

Node 1

The configuration for node 1 is the same as described in the “Node 1” section on page 10-47.

Node 2

Figure 10-34 shows the shelf configuration for node 2 in the splitter protected meshed ring with unprotected channels shown in Figure 10-33 on page 10-63. Slot 2 uses the splitter line card motherboard, which cross connects the signal to the add/drop mux/demux modules in subslot 0 of both west and east mux/demux slots 0 and 1. Slot 4, which supports the unprotected channels, uses a nonsplitter line card motherboard.

Figure 10-34 Shelf Configuration for Node 2 in Splitter Protected Meshed Ring with Unprotected Channels

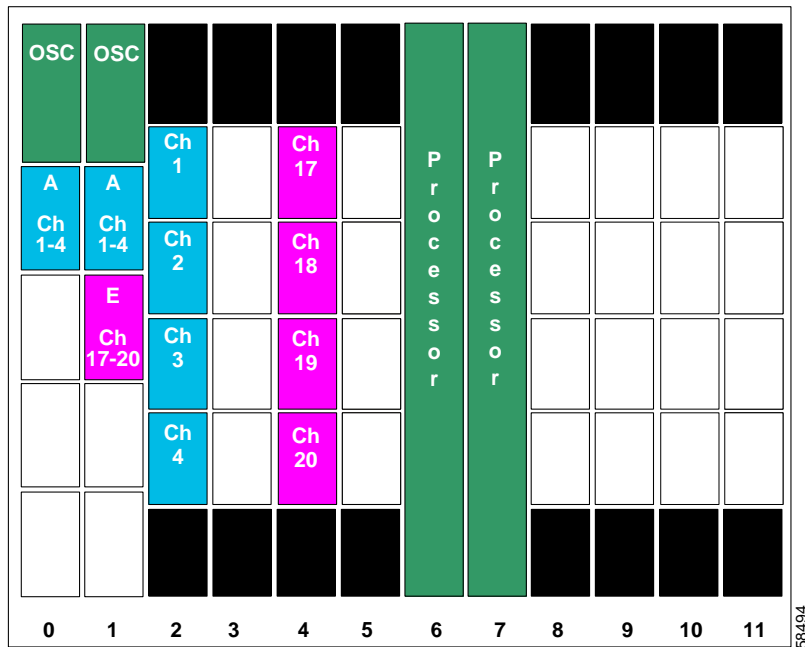
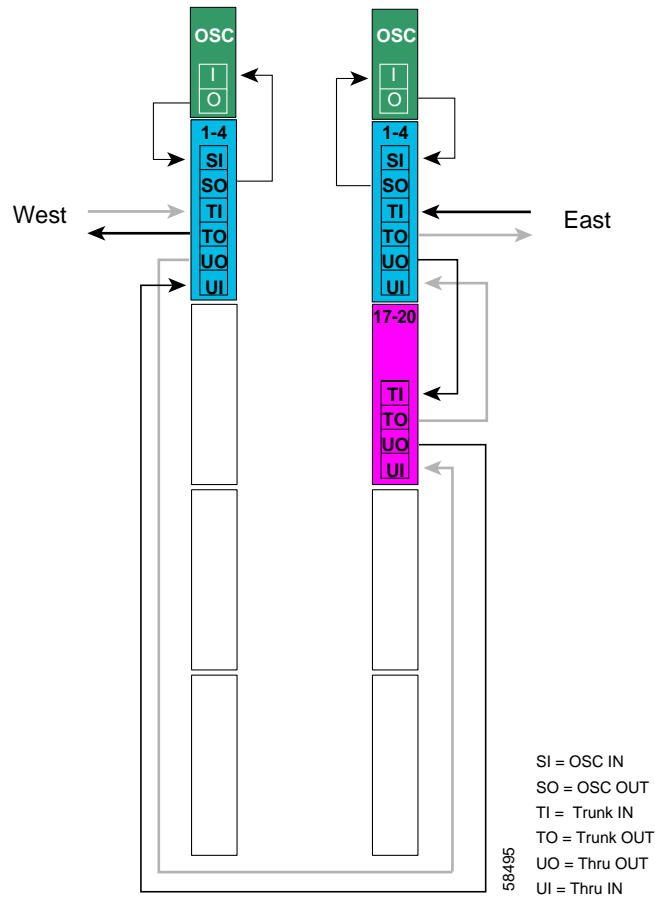


Figure 10-35 shows how the 4-channel mux/demux modules are cabled for node 2 in the splitter protected meshed ring with unprotected channel shown in Figure 10-33 on page 10-63.

Figure 10-35 Add/Drop Mux/Demux Module Cabling for Node 2 in Splitter Protected Meshed Ring with Unprotected Channels



Patch Connections

```

Node2# configure terminal
Node2(config)# patch thru 0/0 thru 1/1
Node2(config)# patch wdm 1/1 thru 1/0
Node2(config)# patch wave 0 oscfilter 0/0
Node2(config)# patch wave 1 oscfilter 1/0

Node2(config)# patch wavepatch 2/0/0 filter 0/0/0
Node2(config)# patch wavepatch 2/1/0 filter 0/0/1
Node2(config)# patch wavepatch 2/2/0 filter 0/0/2
Node2(config)# patch wavepatch 2/3/0 filter 0/0/3
Node2(config)# patch wavepatch 2/0/1 filter 1/0/0
Node2(config)# patch wavepatch 2/1/1 filter 1/0/1
Node2(config)# patch wavepatch 2/2/1 filter 1/0/2
Node2(config)# patch wavepatch 2/3/1 filter 1/0/3

Node2(config)# patch wavepatch 4/0/0 filter 1/1/0
Node2(config)# patch wavepatch 4/1/0 filter 1/1/1

```

```
Node2 (config)# patch wavepatch 4/2/0 filter 1/1/2
Node2 (config)# patch wavepatch 4/3/0 filter 1/1/3
```

Transparent Interfaces in Slot 2

```
Node2 (config)# interface transparent 2/0/0
Node2 (config-if)# encapsulation gigabitethernet
Node2 (config-if)# monitor enable
Node2 (config-if)# exit
```

```
Node2 (config)# interface transparent 2/1/0
Node2 (config-if)# encapsulation gigabitethernet
Node2 (config-if)# monitor enable
Node2 (config-if)# exit
Node2 (config)# interface wave 2/1
Node2 (config-if)# laser frequency 192200
Node2 (config-if)# exit
```

```
Node2 (config)# interface transparent 2/2/0
Node2 (config-if)# encapsulation gigabitethernet
Node2 (config-if)# monitor enable
Node2 (config-if)# exit
```

```
Node2 (config)# interface transparent 2/3/0
Node2 (config-if)# encapsulation gigabitethernet
Node2 (config-if)# monitor enable
Node2 (config-if)# exit
Node2 (config)# interface wave 2/3
Node2 (config-if)# laser frequency 192400
Node2 (config-if)# exit
```

Transparent Interfaces in Slot 4

```
Node2 (config)# interface transparent 4/0/0
Node2 (config-if)# encapsulation sonet oc12
Node2 (config-if)# monitor enable
Node2 (config-if)# exit
```

```
Node2 (config)# interface transparent 4/1/0
Node2 (config-if)# encapsulation sonet oc12
Node2 (config-if)# monitor enable
Node2 (config-if)# exit
Node2 (config)# interface wave 4/1
Node2 (config-if)# laser frequency 194200
Node2 (config-if)# exit
```

```
Node2 (config)# interface transparent 4/2/0
Node2 (config-if)# encapsulation sonet oc12
Node2 (config-if)# monitor enable
Node2 (config-if)# exit
```

```
Node2 (config)# interface transparent 4/3/0
Node2 (config-if)# encapsulation sonet oc12
Node2 (config-if)# monitor enable
Node2 (config-if)# exit
Node2 (config)# interface wave 4/3
Node2 (config-if)# laser frequency 194400
Node2 (config-if)# exit
```

OSC Interfaces

```
Node2(config)# interface wave 0
Node2(config-if)# no shutdown
Node2(config-if)# exit

Node2(config)# interface wave 1
Node2(config-if)# no shutdown
Node2(config-if)# exit
```

APS

```
Node2(config)# redundancy
Node2(config-red)# associate group channel1
Node2(config-red-aps)# aps working wavepatch 2/0/0
Node2(config-red-aps)# aps protection wavepatch 2/0/1
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# exit
Node2(config-red)# associate group channel2
Node2(config-red-aps)# aps working wavepatch 2/1/0
Node2(config-red-aps)# aps protection wavepatch 2/1/1
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# exit
Node2(config-red)# associate group channel3
Node2(config-red-aps)# aps working wavepatch 2/2/0
Node2(config-red-aps)# aps protection wavepatch 2/2/1
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# exit
Node2(config-red)# associate group channel4
Node2(config-red-aps)# aps working wavepatch 2/3/0
Node2(config-red-aps)# aps protection wavepatch 2/3/1
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# end

Node2# copy system:running-config nvram:startup-config
```

Node 3

Figure 10-36 shows the shelf configuration for node 3 in the splitter protected meshed ring with unprotected channels shown in Figure 10-33 on page 10-63. Slot 5 and slot 11 use splitter line card motherboards, which cross connect the signal to the add/drop mux/demux modules in subslot 1 and subslot 3, respectively, of both west and east mux/demux slots 0 and 1. Slot 8, which supports the unprotected channels, uses a nonsplitter line card motherboard.

Figure 10-36 Shelf Configuration for Node 3 in Splitter Protected Meshed Ring with Unprotected Channels

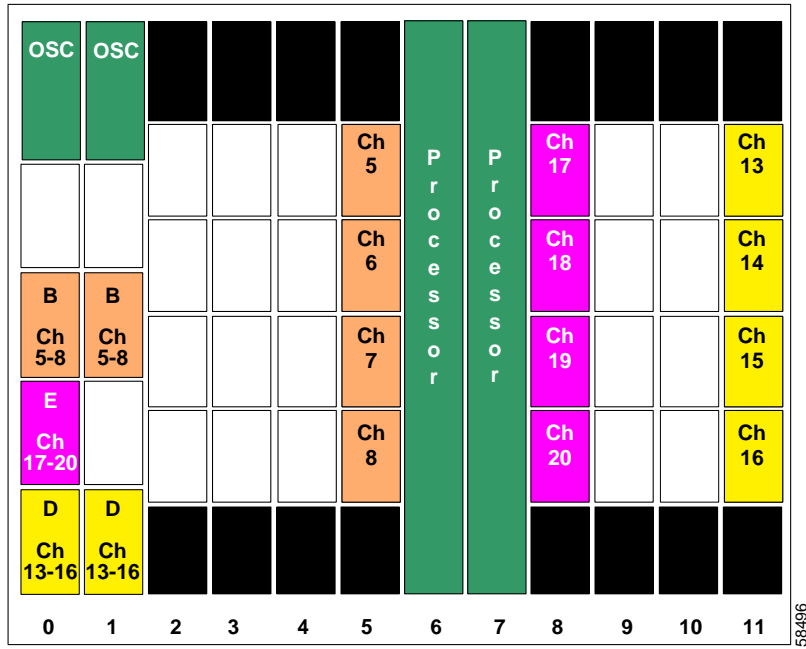
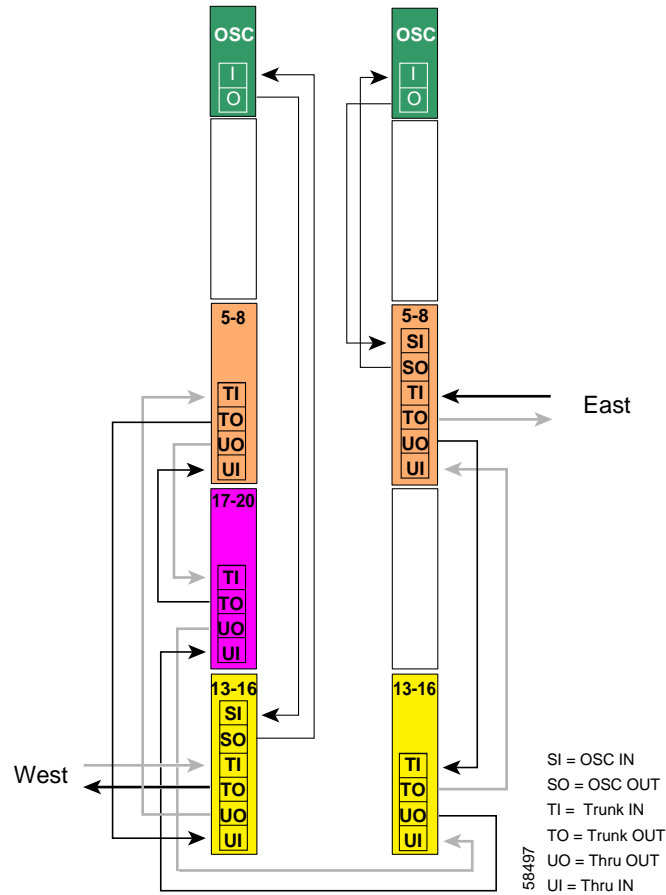


Figure 10-37 shows how the 4-channel mux/demux modules are cabled for node 3 in the splitter protected meshed ring with unprotected channels shown in Figure 10-33 on page 10-63.

Figure 10-37 Add/Drop Mux/Demux Module Cabling for Node 3 in Splitter Protected Meshed Ring with Unprotected Channels



Patch Connections

```

Node3# configure terminal
Node3(config)# patch thru 0/3 wdm 0/1
Node3(config)# patch thru 0/1 wdm 0/2
Node3(config)# patch thru 0/2 thru 1/3
Node3(config)# patch wdm 1/3 thru 1/1
Node3(config)# patch wave 0 oscfilter 0/3
Node3(config)# patch wave 1 oscfilter 1/1

Node3(config)# patch wavepatch 5/0/0 filter 0/1/0
Node3(config)# patch wavepatch 5/1/0 filter 0/1/1
Node3(config)# patch wavepatch 5/2/0 filter 0/1/2
Node3(config)# patch wavepatch 5/3/0 filter 0/1/3
Node3(config)# patch wavepatch 5/0/1 filter 1/1/0
Node3(config)# patch wavepatch 5/1/1 filter 1/1/1
Node3(config)# patch wavepatch 5/2/1 filter 1/1/2
Node3(config)# patch wavepatch 5/3/1 filter 1/1/3
  
```

```

Node3 (config)# patch wavepatch 8/0/0 filter 0/2/0
Node3 (config)# patch wavepatch 8/1/0 filter 0/2/1
Node3 (config)# patch wavepatch 8/2/0 filter 0/2/2
Node3 (config)# patch wavepatch 8/3/0 filter 0/2/3

Node3 (config)# patch wavepatch 11/0/0 filter 0/3/0
Node3 (config)# patch wavepatch 11/1/0 filter 0/3/1
Node3 (config)# patch wavepatch 11/2/0 filter 0/3/2
Node3 (config)# patch wavepatch 11/3/0 filter 0/3/3
Node3 (config)# patch wavepatch 11/0/1 filter 1/3/0
Node3 (config)# patch wavepatch 11/1/1 filter 1/3/1
Node3 (config)# patch wavepatch 11/2/1 filter 1/3/2
Node3 (config)# patch wavepatch 11/3/1 filter 1/3/3

```

Transparent Interfaces in Slot 5

```

Node3 (config)# interface transparent 5/0/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit

Node3 (config)# interface transparent 5/1/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit
Node3 (config)# interface wave 5/1
Node3 (config-if)# laser frequency 192700
Node3 (config-if)# exit

Node3 (config)# interface transparent 5/2/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit

Node3 (config)# interface transparent 5/3/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit
Node3 (config)# interface wave 5/3
Node3 (config-if)# laser frequency 192900
Node3 (config-if)# exit

```

Transparent Interfaces in Slot 8

```

Node3 (config)# interface transparent 4/0/0
Node3 (config-if)# encapsulation sonet oc12
Node3 (config-if)# monitor enable
Node3 (config-if)# exit

Node3 (config)# interface transparent 4/1/0
Node3 (config-if)# encapsulation sonet oc12
Node3 (config-if)# monitor enable
Node3 (config-if)# exit
Node3 (config)# interface wave 4/1
Node3 (config-if)# laser frequency 194200
Node3 (config-if)# exit

Node3 (config)# interface transparent 4/2/0
Node3 (config-if)# encapsulation sonet oc12

```



```
Node3(config-if)# monitor enable
Node3(config-if)# exit

Node3(config)# interface transparent 4/3/0
Node3(config-if)# encapsulation sonet oc12
Node3(config-if)# monitor enable
Node3(config-if)# exit
Node3(config)# interface wave 4/3
Node3(config-if)# laser frequency 194400
Node3(config-if)# exit
```

Transparent Interfaces in Slot 11

```
Node3(config)# interface transparent 11/0/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit

Node3(config)# interface transparent 11/1/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
Node3(config)# interface wave 11/1
Node3(config-if)# laser frequency 1953700
Node3(config-if)# exit

Node3(config)# interface transparent 11/2/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit

Node3(config)# interface transparent 11/3/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
Node3(config)# interface wave 11/3
Node3(config-if)# laser frequency 193900
Node3(config-if)# exit
```

OSC Interfaces

```
Node3(config)# interface wave 0
Node3(config-if)# no shutdown
Node3(config-if)# exit

Node3(config)# interface wave 1
Node3(config-if)# no shutdown
Node3(config-if)# exit
```

APS

```
Node3(config)# redundancy
Node3(config-red)# associate group channel5
Node3(config-red-aps)# aps working wavepatch 5/0/0
Node3(config-red-aps)# aps protection wavepatch 5/0/1
Node3(config-red-aps)# aps enable
Node3(config-red-aps)# exit
```

```

Node3 (config-red)# associate group channel6
Node3 (config-red-aps)# aps working wavepatch 5/1/0
Node3 (config-red-aps)# aps protection wavepatch 5/1/1
Node3 (config-red-aps)# aps enable
Node3 (config-red-aps)# exit
Node3 (config-red)# associate group channel7
Node3 (config-red-aps)# aps working wavepatch 5/2/0
Node3 (config-red-aps)# aps protection wavepatch 5/2/1
Node3 (config-red-aps)# aps enable
Node3 (config-red-aps)# exit
Node3 (config-red)# associate group channel8
Node3 (config-red-aps)# aps working wavepatch 5/3/0
Node3 (config-red-aps)# aps protection wavepatch 5/3/1
Node3 (config-red-aps)# aps enable
Node3 (config-red-aps)# exit

Node3 (config-red)# associate group channel13
Node3 (config-red-aps)# aps working wavepatch 11/0/1
Node3 (config-red-aps)# aps protection wavepatch 11/0/0
Node3 (config-red-aps)# aps enable
Node3 (config-red-aps)# exit
Node3 (config-red)# associate group channel14
Node3 (config-red-aps)# aps working wavepatch 11/1/1
Node3 (config-red-aps)# aps protection wavepatch 11/1/0
Node3 (config-red-aps)# aps enable
Node3 (config-red-aps)# exit
NNode3 (config-red)# associate group channel15
Node3 (config-red-aps)# aps working wavepatch 11/2/1
Node3 (config-red-aps)# aps protection wavepatch 11/2/0
Node3 (config-red-aps)# aps enable
Node3 (config-red-aps)# exit
Node3 (config-red)# associate group channel16
Node3 (config-red-aps)# aps working wavepatch 11/3/1
Node3 (config-red-aps)# aps protection wavepatch 11/3/0
Node3 (config-red-aps)# aps enable
Node3 (config-red-aps)# end

Node3# copy system:running-config nvram:startup-config

```

Node 4

The configuration for node 4 is the same as described in the “Node 4” section on page 10-59.

Configuring a Meshed Ring with Line Card Protection and OSC

Line card protection requires different shelf and CLI configuration from splitter protection. The following sections describe an example based on the meshed ring topology shown in Figure 10-24 on page 10-46.

Node 1

Figure 10-38 shows the shelf configuration for node 1 using line card protection in the example meshed ring shown in Figure 10-24 on page 10-46. Slots 2, 5, and 8 use nonsplitter line card motherboards that cross connect the signal to the add/drop mux/demux modules in the west mux/demux slot 0; slots 3, 4, and 10 use nonsplitter line card motherboards that cross connects the signal to the add/drop mux/demux modules in the east mux/demux slot 1.

Figure 10-38 Shelf Configuration for Node 1 in Line Card Protected Meshed Ring

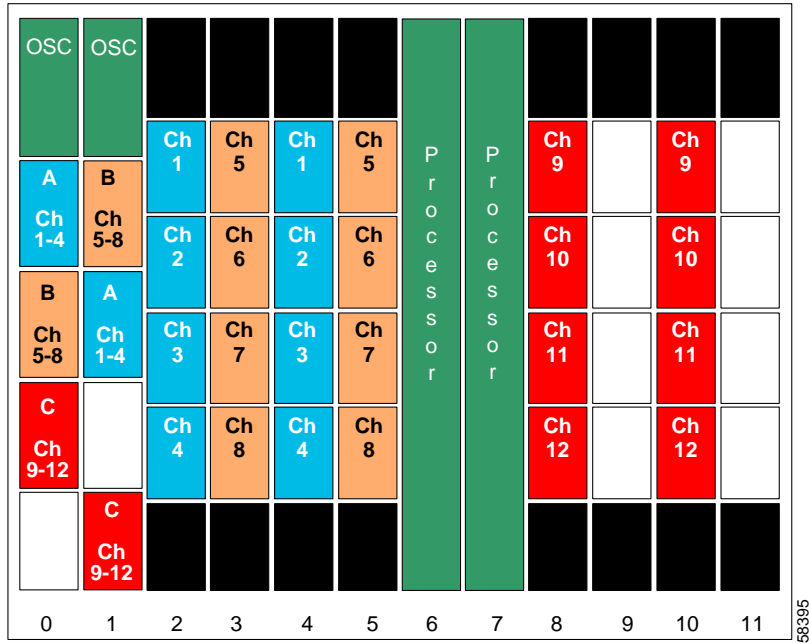
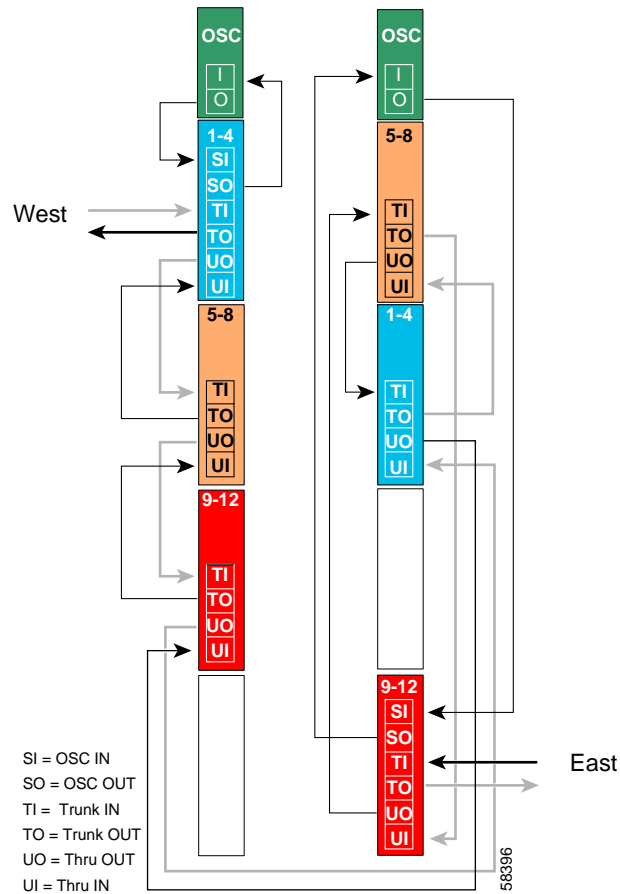


Figure 10-39 shows how the 4-channel mux/demux modules are cabled for node 1 in the line card protected meshed ring shown in Figure 10-24 on page 10-46.

Figure 10-39 Add/Drop Mux/Demux Module Cabling with OSC for Node 1 in Line Card Protected Meshed Ring



Patch Connections

```

Node1# configure terminal
Node1(config)# patch thru 0/0 wdm 0/1
Node1(config)# patch thru 0/1 wdm 0/2
Node1(config)# patch thru 0/2 thru 1/1
Node1(config)# patch wdm 1/1 thru 1/0
Node1(config)# patch wdm 1/0 thru 1/3
Node1(config)# patch wave 0 oscfilter 0/0
Node1(config)# patch wave 1 oscfilter 1/3

Node1(config)# patch wavepatch 2/0/0 filter 0/0/0
Node1(config)# patch wavepatch 2/1/0 filter 0/0/1
Node1(config)# patch wavepatch 2/2/0 filter 0/0/2
Node1(config)# patch wavepatch 2/3/0 filter 0/0/3

Node1(config)# patch wavepatch 3/0/0 filter 1/0/0
Node1(config)# patch wavepatch 3/1/0 filter 1/0/1
Node1(config)# patch wavepatch 3/2/0 filter 1/0/2
Node1(config)# patch wavepatch 3/3/0 filter 1/0/3

```

```
Node1(config)# patch wavepatch 4/0/0 filter 1/1/0
Node1(config)# patch wavepatch 4/1/0 filter 1/1/1
Node1(config)# patch wavepatch 4/2/0 filter 1/1/2
Node1(config)# patch wavepatch 4/3/0 filter 1/1/3

Node1(config)# patch wavepatch 5/0/0 filter 0/1/0
Node1(config)# patch wavepatch 5/1/0 filter 0/1/1
Node1(config)# patch wavepatch 5/2/0 filter 0/1/2
Node1(config)# patch wavepatch 5/3/0 filter 0/1/3

Node1(config)# patch wavepatch 8/0/0 filter 0/2/0
Node1(config)# patch wavepatch 8/1/0 filter 0/2/1
Node1(config)# patch wavepatch 8/2/0 filter 0/2/2
Node1(config)# patch wavepatch 8/3/0 filter 0/2/3

Node1(config)# patch wavepatch 10/0/0 filter 1/3/0
Node1(config)# patch wavepatch 10/1/0 filter 1/3/1
Node1(config)# patch wavepatch 10/2/0 filter 1/3/2
Node1(config)# patch wavepatch 10/3/0 filter 1/3/3
```

Transparent Interfaces in Slot 2

```
Node1(config)# interface transparent 2/0/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 2/1/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 2/1
Node1(config-if)# laser frequency 192200
Node1(config-if)# exit

Node1(config)# interface transparent 2/2/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 2/3/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 2/3
Node1(config-if)# laser frequency 192400
Node1(config-if)# exit
```

Transparent Interfaces in Slot 3

```
Node1(config)# interface transparent 3/0/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 3/1/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
```

```

Node1(config-if)# exit
Node1(config)# interface wave 3/1
Node1(config-if)# laser frequency 192700
Node1(config-if)# exit

Node1(config)# interface transparent 3/2/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 3/3/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 3/3
Node1(config-if)# laser frequency 192900
Node1(config-if)# exit

```

Transparent Interfaces in Slot 4

```

Node1(config)# interface transparent 4/0/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 4/1/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 4/1
Node1(config-if)# laser frequency 192200
Node1(config-if)# exit

Node1(config)# interface transparent 4/2/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 4/3/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 4/3
Node1(config-if)# laser frequency 192400
Node1(config-if)# exit

```

Transparent Interfaces in Slot 5

```

Node1(config)# interface transparent 5/0/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 5/1/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 5/1
Node1(config-if)# laser frequency 192700

```

```
Node1(config-if)# exit

Node1(config)# interface transparent 5/2/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 5/3/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 5/3
Node1(config-if)# laser frequency 192900
Node1(config-if)# exit
```

Transparent Interfaces in Slot 8

```
Node1(config)# interface transparent 8/0/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 8/1/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 8/1
Node1(config-if)# laser frequency 193200
Node1(config-if)# exit

Node1(config)# interface transparent 8/2/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 8/3/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 8/3
Node1(config-if)# laser frequency 193400
Node1(config-if)# exit
```

Transparent Interfaces in Slot 10

```
Node1(config)# interface transparent 10/0/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 10/1/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 10/1
Node1(config-if)# laser frequency 193200
Node1(config-if)# exit

Node1(config)# interface transparent 10/2/0
```

```

Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

Node1(config)# interface transparent 10/3/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
Node1(config)# interface wave 10/3
Node1(config-if)# laser frequency 193400
Node1(config-if)# exit

```

OSC Interfaces

```

Node1(config)# interface wave 0
Node1(config-if)# no shutdown
Node1(config-if)# exit

```

```

Node1(config)# interface wave 1
Node1(config-if)# no shutdown
Node1(config-if)# exit

```

APS

Use the following for configuring y-cable protection.

```

Node1(config)# redundancy
Node1(config-red)# associate group channel1
Node1(config-red-aps)# aps working transparent 4/0/0
Node1(config-red-aps)# aps protection transparent 2/0/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps revertive
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel2
Node1(config-red-aps)# aps working transparent 4/1/0
Node1(config-red-aps)# aps protection transparent 2/1/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps revertive
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel3
Node1(config-red-aps)# aps working transparent 4/2/0
Node1(config-red-aps)# aps protection transparent 2/2/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps revertive
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel4
Node1(config-red-aps)# aps working transparent 4/3/0
Node1(config-red-aps)# aps protection transparent 2/3/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps revertive
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit

Node1(config-red)# associate group channel5
Node1(config-red-aps)# aps working transparent 5/0/0
Node1(config-red-aps)# aps protection transparent 3/0/0

```



```
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps revertive
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel6
Node1(config-red-aps)# aps working transparent 5/1/0
Node1(config-red-aps)# aps protection transparent 3/1/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps revertive
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel7
Node1(config-red-aps)# aps working transparent 5/2/0
Node1(config-red-aps)# aps protection transparent 3/2/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps revertive
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel8
Node1(config-red-aps)# aps working transparent 5/3/0
Node1(config-red-aps)# aps protection transparent 3/3/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps revertive
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit

Node1(config-red)# associate group channel9
Node1(config-red-aps)# aps working transparent 8/0/0
Node1(config-red-aps)# aps protection transparent 11/0/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps revertive
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel10
Node1(config-red-aps)# aps working transparent 8/1/0
Node1(config-red-aps)# aps protection transparent 11/1/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps revertive
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel11
Node1(config-red-aps)# aps working transparent 8/2/0
Node1(config-red-aps)# aps protection transparent 11/2/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps revertive
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1(config-red)# associate group channel12
Node1(config-red-aps)# aps working transparent 8/3/0
Node1(config-red-aps)# aps protection transparent 11/3/0
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps revertive
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# end

Node1# copy system:running-config nvram:startup-config
```

Node 2

Figure 10-40 shows the shelf configuration for node 2 in the line card protected meshed ring shown in Figure 10-24 on page 10-46. Slot 2 uses the nonsplitter line card motherboard that cross connects the signal to the add/drop mux/demux module in the west mux/demux slot 0; slot 4 uses the nonsplitter line card motherboard that cross connects the signal to the add/drop mux/demux module in the east mux/demux slot 1.

Figure 10-40 Shelf Configuration for Node 2 in Line Card Protected Meshed Ring

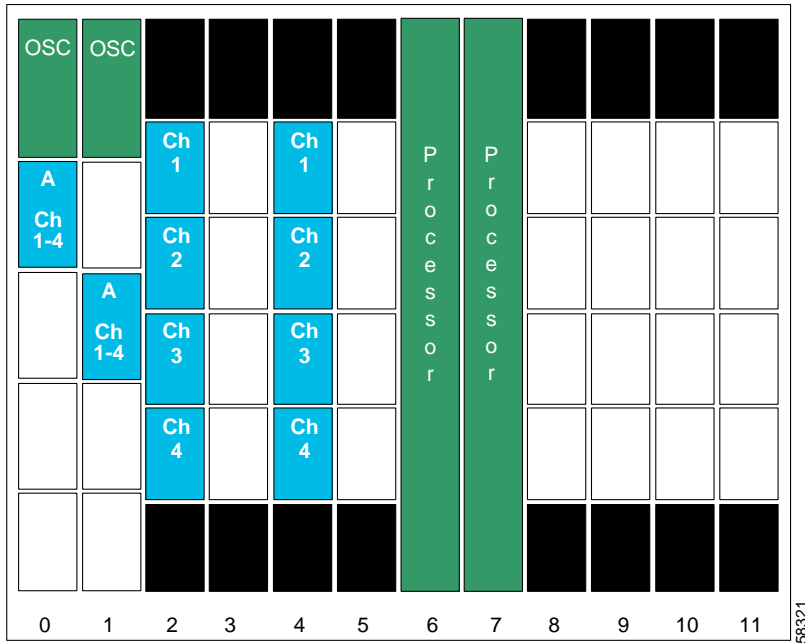
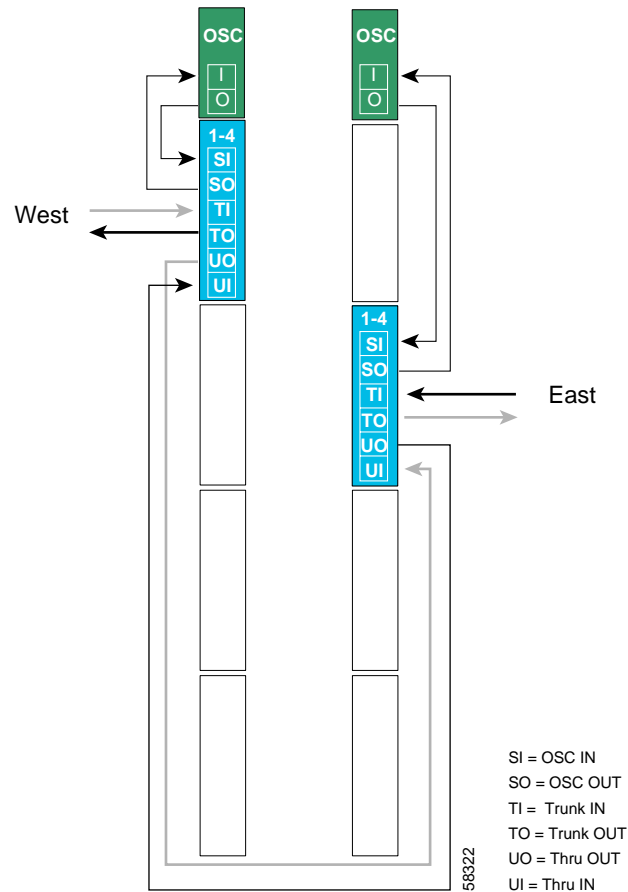


Figure 10-41 shows how the 4-channel mux/demux modules are cabled for node 2 in the line card protected meshed ring shown in Figure 10-24 on page 10-46.

Figure 10-41 Add/Drop Mux/Demux Module Cabling with OSC for Node 2 in Line Card Protected Meshed Ring



Patch Connections

```
Node2# configure terminal
Node2(config)# patch thru 0/0 thru 1/1
Node2(config)# patch wave 0 oscfilter 0/0
Node2(config)# patch wave 1 oscfilter 1/1

Node2(config)# patch wavepatch 2/0/0 filter 0/0/0
Node2(config)# patch wavepatch 2/1/0 filter 0/0/1
Node2(config)# patch wavepatch 2/2/0 filter 0/0/2
Node2(config)# patch wavepatch 2/3/0 filter 0/0/3

Node2(config)# patch wavepatch 4/0/0 filter 1/1/0
Node2(config)# patch wavepatch 4/1/0 filter 1/1/1
Node2(config)# patch wavepatch 4/2/0 filter 1/1/2
Node2(config)# patch wavepatch 4/3/0 filter 1/1/3
```

Transparent Interfaces in Slot 2

```
Node2(config)# interface transparent 2/0/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 2/1/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
Node2(config)# interface wave 2/1
Node2(config-if)# laser frequency 192200
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 2/2/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 2/3/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
Node2(config)# interface wave 2/3
Node2(config-if)# laser frequency 192400
Node2(config-if)# exit
```

Transparent Interfaces in Slot 4

```
Node2(config)# interface transparent 4/0/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 4/1/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
Node2(config)# interface wave 4/1
Node2(config-if)# laser frequency 192200
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 4/2/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 4/3/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
Node2(config)# interface wave 4/3
Node2(config-if)# laser frequency 192400
Node2(config-if)# exit
```

OSC Interfaces

```
Node2(config)# interface wave 0
Node2(config-if)# no shutdown
```

```
Node2(config-if)# exit

Node2(config)# interface wave 1
Node2(config-if)# no shutdown
Node2(config-if)# exit
```

APS

Use the following for configuring y-cable protection.

```
Node2(config)# redundancy
Node2(config-red)# associate group channel1
Node2(config-red-aps)# aps working transparent 2/0/0
Node2(config-red-aps)# aps protection transparent 4/0/0
Node2(config-red-aps)# aps y-cable
Node2(config-red-aps)# aps revertive
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# exit
Node2(config-red)# associate group channel2
Node2(config-red-aps)# aps working transparent 2/1/0
Node2(config-red-aps)# aps protection transparent 4/1/0
Node2(config-red-aps)# aps y-cable
Node2(config-red-aps)# aps revertive
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# exit
Node2(config-red)# associate group channel3
Node2(config-red-aps)# aps working transparent 2/2/0
Node2(config-red-aps)# aps protection transparent 4/2/0
Node2(config-red-aps)# aps y-cable
Node2(config-red-aps)# aps revertive
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# exit
Node2(config-red)# associate group channel4
Node2(config-red-aps)# aps working transparent 2/3/0
Node2(config-red-aps)# aps protection transparent 4/3/0
Node2(config-red-aps)# aps y-cable
Node2(config-red-aps)# aps revertive
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# end

Node2# copy system:running-config nvram:startup-config
```

Node 3

Figure 10-42 shows the shelf configuration for node 3 in the line card protected meshed ring shown in Figure 10-24 on page 10-46. Slots 5 and 11 use the nonsplitter line card motherboards, that cross connects the signal to the add/drop mux/demux modules in the west mux/demux slot 0; slots 3 and 9 use the nonsplitter line card motherboards that cross connects to the add/drop mux/demux modules in the east mux/demux slot 1.

Figure 10-42 Shelf Configuration for Node 3 in Line Card Protected Meshed Ring

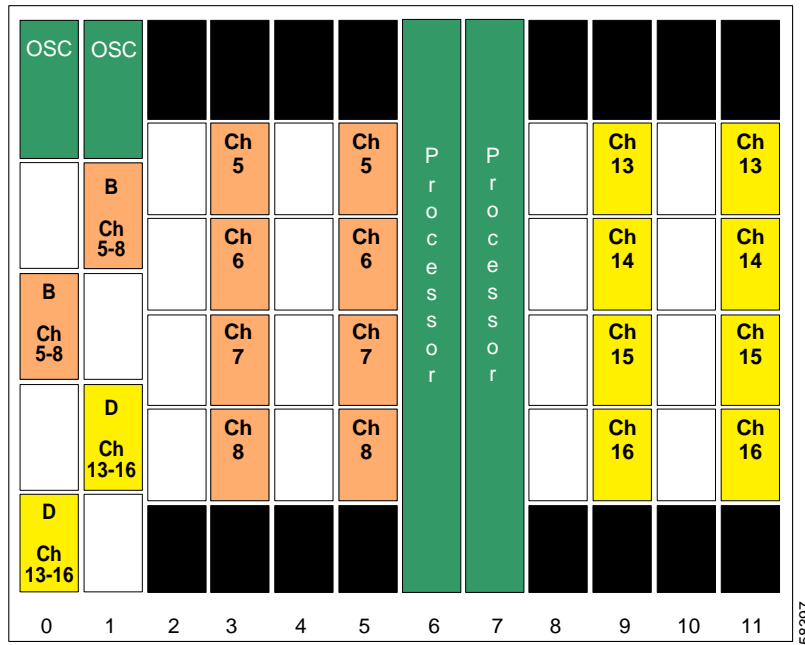
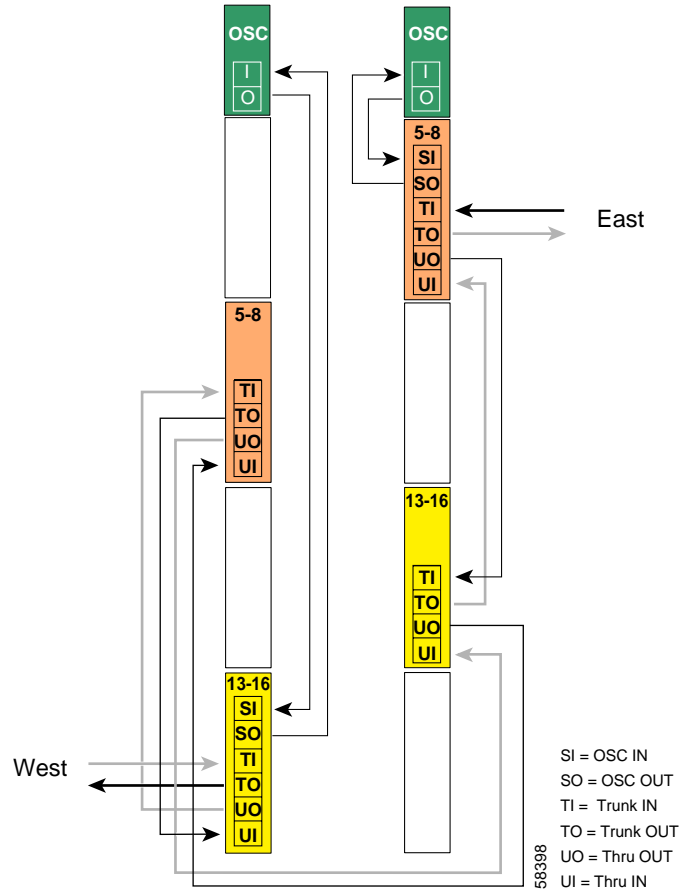


Figure 10-43 shows how the 4-channel mux/demux modules are cabled for the line card protected meshed ring shown in Figure 10-24 on page 10-46.

Figure 10-43 Add/Drop Mux/Demux Module Cabling with OSC for Node 3 in Line Card Protected Meshed Ring



Patch Connections

```

Node3# configure terminal
Node3(config)# patch thru 0/1 wdm 0/3
Node3(config)# patch thru 0/3 thru 1/0
Node3(config)# patch wdm 1/0 thru 1/2
Node3(config)# patch wave 0 oscfilter 0/3
Node3(config)# patch wave 1 oscfilter 1/0

Node3(config)# patch wavepatch 3/0/0 filter 0/1/0
Node3(config)# patch wavepatch 3/1/0 filter 0/1/1
Node3(config)# patch wavepatch 3/2/0 filter 0/1/2
Node3(config)# patch wavepatch 3/3/0 filter 0/1/3

Node3(config)# patch wavepatch 5/0/0 filter 1/0/0
Node3(config)# patch wavepatch 5/1/0 filter 1/0/1
Node3(config)# patch wavepatch 5/2/0 filter 1/0/2
Node3(config)# patch wavepatch 5/3/0 filter 1/0/3
  
```

```

Node3 (config)# patch wavepatch 9/0/0 filter 0/3/0
Node3 (config)# patch wavepatch 9/1/0 filter 0/3/1
Node3 (config)# patch wavepatch 9/2/0 filter 0/3/2
Node3 (config)# patch wavepatch 9/3/0 filter 0/3/3

Node3 (config)# patch wavepatch 11/0/0 filter 1/2/0
Node3 (config)# patch wavepatch 11/1/0 filter 1/2/1
Node3 (config)# patch wavepatch 11/2/0 filter 1/2/2
Node3 (config)# patch wavepatch 11/3/0 filter 1/2/3

```

Transparent Interfaces in Slot 3

```

Node3 (config)# interface transparent 3/0/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit

Node3 (config)# interface transparent 3/1/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit
Node3 (config)# interface wave 3/1
Node3 (config-if)# laser frequency 192700
Node3 (config-if)# exit

Node3 (config)# interface transparent 3/2/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit

Node3 (config)# interface transparent 3/3/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit
Node3 (config)# interface wave 3/3
Node3 (config-if)# laser frequency 192900
Node3 (config-if)# exit

```

Transparent Interfaces in Slot 5

```

Node3 (config)# interface transparent 5/0/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit

Node3 (config)# interface transparent 5/1/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit
Node3 (config)# interface wave 5/1
Node3 (config-if)# laser frequency 192700
Node3 (config-if)# exit

Node3 (config)# interface transparent 5/2/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit

Node3 (config)# interface transparent 5/3/0

```



```
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
Node3(config)# interface wave 5/3
Node3(config-if)# laser frequency 192900
Node3(config-if)# exit
```

Transparent Interfaces in Slot 9

```
Node3(config)# interface transparent 9/0/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
```

```
Node3(config)# interface transparent 9/1/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
Node3(config)# interface wave 9/1
Node3(config-if)# laser frequency 1953700
Node3(config-if)# exit
```

```
Node3(config)# interface transparent 9/2/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
```

```
Node3(config)# interface transparent 9/3/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
Node3(config)# interface wave 9/3
Node3(config-if)# laser frequency 193900
Node3(config-if)# exit
```

Transparent Interfaces in Slot 11

```
Node3(config)# interface transparent 11/0/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
```

```
Node3(config)# interface transparent 11/1/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
Node3(config)# interface wave 11/1
Node3(config-if)# laser frequency 1953700
Node3(config-if)# exit
```

```
Node3(config)# interface transparent 11/2/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
```

```
Node3(config)# interface transparent 11/3/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
```

```

Node3 (config)# interface wave 11/3
Node3 (config-if)# laser frequency 193900
Node3 (config-if)# exit

```

OSC Interfaces

```

Node3 (config)# interface wave 0
Node3 (config-if)# no shutdown
Node3 (config-if)# exit

```

```

Node3 (config)# interface wave 1
Node3 (config-if)# no shutdown
Node3 (config-if)# exit

```

APS

Use the following for configuring y-cable protection.

```

Node3 (config)# redundancy
Node3 (config-red)# associate group channel5
Node3 (config-red-aps)# aps working transparent 3/0/0
Node3 (config-red-aps)# aps protection transparent 5/0/0
Node3 (config-red-aps)# aps y-cable
Node3 (config-red-aps)# aps revertive
Node3 (config-red-aps)# aps enable
Node3 (config-red-aps)# exit
Node3 (config-red)# associate group channel6
Node3 (config-red-aps)# aps working transparent 3/1/0
Node3 (config-red-aps)# aps protection transparent 5/1/0
Node3 (config-red-aps)# aps y-cable
Node3 (config-red-aps)# aps revertive
Node3 (config-red-aps)# aps enable
Node3 (config-red-aps)# exit
Node3 (config-red)# associate group channel7
Node3 (config-red-aps)# aps working transparent 3/2/0
Node3 (config-red-aps)# aps protection transparent 5/2/0
Node3 (config-red-aps)# aps y-cable
Node3 (config-red-aps)# aps revertive
Node3 (config-red-aps)# aps enable
Node3 (config-red-aps)# exit
Node3 (config-red)# associate group channel8
Node3 (config-red-aps)# aps working transparent 3/3/0
Node3 (config-red-aps)# aps protection transparent 5/3/0
Node3 (config-red-aps)# aps y-cable
Node3 (config-red-aps)# aps revertive
Node3 (config-red-aps)# aps enable
Node3 (config-red-aps)# exit
Node3 (config-red)# associate group channel13
Node3 (config-red-aps)# aps working transparent 11/0/0
Node3 (config-red-aps)# aps protection transparent 9/0/0
Node3 (config-red-aps)# aps y-cable
Node3 (config-red-aps)# aps revertive
Node3 (config-red-aps)# aps enable
Node3 (config-red-aps)# exit
Node3 (config-red)# associate group channel14
Node3 (config-red-aps)# aps working transparent 11/1/0
Node3 (config-red-aps)# aps protection transparent 9/1/0
Node3 (config-red-aps)# aps y-cable

```

```

Node3(config-red-aps)# aps revertive
Node3(config-red-aps)# aps enable
Node3(config-red-aps)# exit
Node3(config-red)# associate group channel15
Node3(config-red-aps)# aps working transparent 11/2/0
Node3(config-red-aps)# aps protection transparent 9/2/0
Node3(config-red-aps)# aps y-cable
Node3(config-red-aps)# aps revertive
Node3(config-red-aps)# aps enable
Node3(config-red-aps)# exit
Node3(config-red)# associate group channel16
Node3(config-red-aps)# aps working transparent 11/3/0
Node3(config-red-aps)# aps protection transparent 9/3/0
Node3(config-red-aps)# aps y-cable
Node3(config-red-aps)# aps revertive
Node3(config-red-aps)# aps enable
Node3(config-red-aps)# end

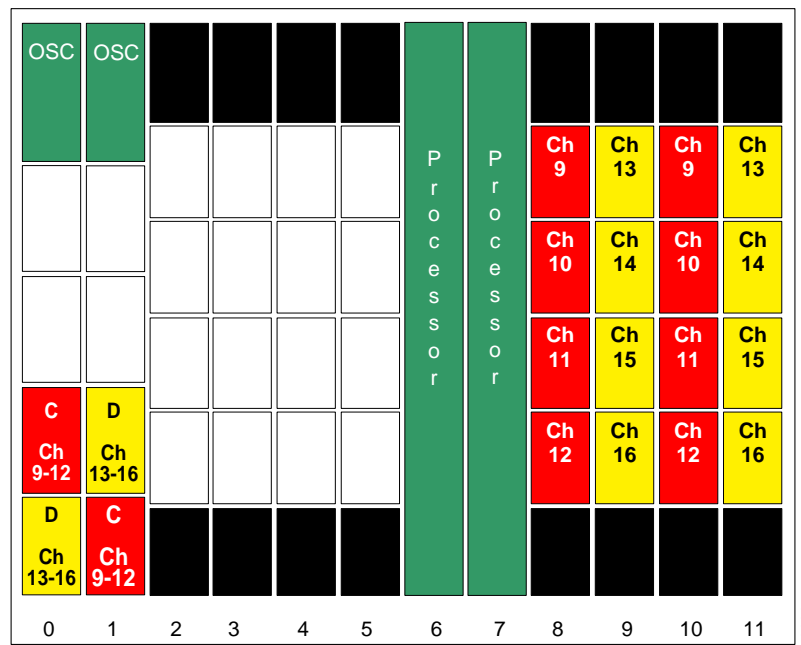
Node3# copy system:running-config nvram:startup-config

```

Node 4

Figure 10-44 shows the shelf configuration for node 4 in the line card protected meshed ring shown in Figure 10-24 on page 10-46. Slots 8 and 11 use the nonsplitter line card motherboards that cross connects the signal to the add/drop mux/demux modules in the west mux/demux slots 0; slots 9 and 10 use the nonsplitter line card motherboards that cross connects the signal to the add/drop mux/demux modules in the east mux/demux slot 1.

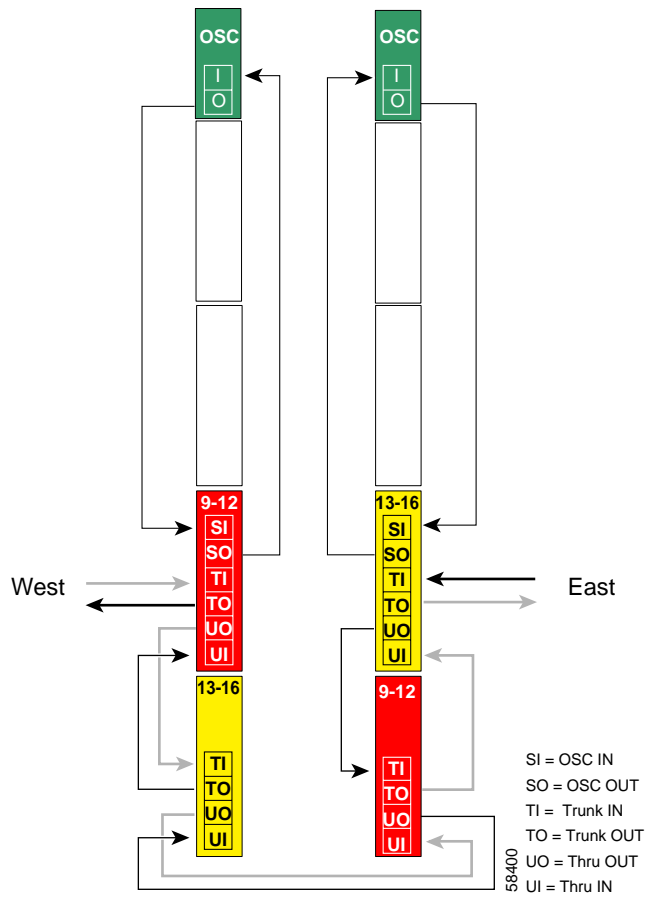
Figure 10-44 Shelf Configuration for Node 4 in Line Card Protected Meshed Ring



58399

Figure 10-45 shows how the 4-channel mux/demux modules are cabled for node 4 in the line card protected meshed ring shown in Figure 10-24 on page 10-46.

Figure 10-45 Add/Drop Mux/Demux Module Cabling with OSC for Node 4 in Line Card Protected Meshed Ring



Patch Connections

```

Node4# configure terminal
Node4 (config)# patch thru 0/2 wdm 0/3
Node4 (config)# patch thru 0/3 thru 1/3
Node4 (config)# patch wdm 1/3 thru 1/2
Node4 (config)# patch wave 0 oscfilter 0/2
Node4 (config)# patch wave 1 oscfilter 1/2

Node4 (config)# patch wavepatch 8/0/0 filter 0/2/0
Node4 (config)# patch wavepatch 8/1/0 filter 0/2/1
Node4 (config)# patch wavepatch 8/2/0 filter 0/2/2
Node4 (config)# patch wavepatch 8/3/0 filter 0/2/3

Node4 (config)# patch wavepatch 9/0/0 filter 1/2/0
Node4 (config)# patch wavepatch 9/1/0 filter 1/2/1
Node4 (config)# patch wavepatch 9/2/0 filter 1/2/2
Node4 (config)# patch wavepatch 9/3/0 filter 1/2/3
  
```

```
Node4(config)# patch wavepatch 10/0/0 filter 1/3/0
Node4(config)# patch wavepatch 10/1/0 filter 1/3/1
Node4(config)# patch wavepatch 10/2/0 filter 1/3/2
Node4(config)# patch wavepatch 10/3/0 filter 1/3/3

Node4(config)# patch wavepatch 11/0/0 filter 0/3/0
Node4(config)# patch wavepatch 11/1/0 filter 0/3/1
Node4(config)# patch wavepatch 11/2/0 filter 0/3/2
Node4(config)# patch wavepatch 11/3/0 filter 0/3/3
```

Transparent Interfaces in Slot 8

```
Node4(config)# interface transparent 8/0/0
Node4(config-if)# encapsulation gigabitethernet
Node4(config-if)# monitor enable
Node4(config-if)# exit

Node4(config)# interface transparent 8/1/0
Node4(config-if)# encapsulation gigabitethernet
Node4(config-if)# monitor enable
Node4(config-if)# exit
Node4(config)# interface wave 8/1
Node4(config-if)# laser frequency 193200
Node4(config-if)# exit

Node4(config)# interface transparent 8/2/0
Node4(config-if)# encapsulation gigabitethernet
Node4(config-if)# monitor enable
Node4(config-if)# exit

Node4(config)# interface transparent 8/3/0
Node4(config-if)# encapsulation gigabitethernet
Node4(config-if)# monitor enable
Node4(config-if)# exit
Node4(config)# interface wave 8/3
Node4(config-if)# laser frequency 193400
Node4(config-if)# exit
```

Transparent Interfaces in Slot 9

```
Node4(config)# interface transparent 9/0/0
Node4(config-if)# encapsulation gigabitethernet
Node4(config-if)# monitor enable
Node4(config-if)# exit

Node4(config)# interface transparent 9/1/0
Node4(config-if)# encapsulation gigabitethernet
Node4(config-if)# monitor enable
Node4(config-if)# exit
Node4(config)# interface wave 9/1
Node4(config-if)# laser frequency 1953700
Node4(config-if)# exit

Node4(config)# interface transparent 9/2/0
Node4(config-if)# encapsulation gigabitethernet
Node4(config-if)# monitor enable
Node4(config-if)# exit

Node4(config)# interface transparent 9/3/0
```

```

Node4 (config-if)# encapsulation gigabitethernet
Node4 (config-if)# monitor enable
Node4 (config-if)# exit
Node4 (config)# interface wave 9/3
Node4 (config-if)# laser frequency 193900
Node4 (config-if)# exit

```

Transparent Interfaces in Slot 10

```

Node4 (config)# interface transparent 10/0/0
Node4 (config-if)# encapsulation gigabitethernet
Node4 (config-if)# monitor enable
Node4 (config-if)# exit

```

```

Node4 (config)# interface transparent 10/1/0
Node4 (config-if)# encapsulation gigabitethernet
Node4 (config-if)# monitor enable
Node4 (config-if)# exit
Node4 (config)# interface wave 10/1
Node4 (config-if)# laser frequency 193200
Node4 (config-if)# exit

```

```

Node4 (config)# interface transparent 10/2/0
Node4 (config-if)# encapsulation gigabitethernet
Node4 (config-if)# monitor enable
Node4 (config-if)# exit

```

```

Node4 (config)# interface transparent 10/3/0
Node4 (config-if)# encapsulation gigabitethernet
Node4 (config-if)# monitor enable
Node4 (config-if)# exit
Node4 (config)# interface wave 10/3
Node4 (config-if)# laser frequency 193400
Node4 (config-if)# exit

```

Transparent Interfaces in Slot 11

```

Node4 (config)# interface transparent 11/0/0
Node4 (config-if)# encapsulation gigabitethernet
Node4 (config-if)# monitor enable
Node4 (config-if)# exit

```

```

Node4 (config)# interface transparent 11/1/0
Node4 (config-if)# encapsulation gigabitethernet
Node4 (config-if)# monitor enable
Node4 (config-if)# exit
Node4 (config)# interface wave 11/1
Node4 (config-if)# laser frequency 1953700
Node4 (config-if)# exit

```

```

Node4 (config)# interface transparent 11/2/0
Node4 (config-if)# encapsulation gigabitethernet
Node4 (config-if)# monitor enable
Node4 (config-if)# exit

```

```

Node4 (config)# interface transparent 11/3/0
Node4 (config-if)# encapsulation gigabitethernet
Node4Node4 (config-if)# monitor enable
Node4 (config-if)# exit

```

```

Node4(config)# interface wave 11/3
Node4(config-if)# laser frequency 193900
Node4(config-if)# exit

```

OSC Interfaces

```

Node4(config)# interface wave 0
Node4(config-if)# no shutdown
Node4(config-if)# exit

```

```

Node4(config)# interface wave 1
Node4(config-if)# no shutdown
Node4(config-if)# exit

```

APS

Use the following for configuring y-cable protection.

```

Node4(config)# redundancy
Node4(config-red)# associate group channel9
Node4(config-red-aps)# aps working transparent 10/0/0
Node4(config-red-aps)# aps protection transparent 8/0/0
Node4(config-red-aps)# aps y-cable
Node4(config-red-aps)# aps revertive
Node4(config-red-aps)# aps enable
Node4(config-red-aps)# exit
Node4(config-red)# associate group channel10
Node4(config-red-aps)# aps working transparent 10/1/0
Node4(config-red-aps)# aps protection transparent 8/1/0
Node4(config-red-aps)# aps y-cable
Node4(config-red-aps)# aps revertive
Node4(config-red-aps)# aps enable
Node4(config-red-aps)# exit
Node4(config-red)# associate group channel11
Node4(config-red-aps)# aps working transparent 10/2/0
Node4(config-red-aps)# aps protection transparent 8/2/0
Node4(config-red-aps)# aps y-cable
Node4(config-red-aps)# aps revertive
Node4(config-red-aps)# aps enable
Node4(config-red-aps)# exit
Node4(config-red)# associate group channel12
Node4(config-red-aps)# aps working transparent 10/3/0
Node4(config-red-aps)# aps protection transparent 8/3/0
Node4(config-red-aps)# aps y-cable
Node4(config-red-aps)# aps revertive
Node4(config-red-aps)# aps enable
Node4(config-red-aps)# exit
Node4(config-red)# associate group channel13
Node4(config-red-aps)# aps working transparent 9/0/0
Node4(config-red-aps)# aps protection transparent 11/0/0
Node4(config-red-aps)# aps y-cable
Node4(config-red-aps)# aps revertive
Node4(config-red-aps)# aps enable
Node4(config-red-aps)# exit
Node4(config-red)# associate group channel13
Node4(config-red-aps)# aps working transparent 9/1/0
Node4(config-red-aps)# aps protection transparent 11/1/0
Node4(config-red-aps)# aps y-cable

```

```
Node4 (config-red-aps) # aps revertive
Node4 (config-red-aps) # aps enable
Node4 (config-red-aps) # exit
Node4 (config-red) # associate group channel13
Node4 (config-red-aps) # aps working transparent 9/2/0
Node4 (config-red-aps) # aps protection transparent 11/2/0
Node4 (config-red-aps) # aps y-cable
Node4 (config-red-aps) # aps revertive
Node4 (config-red-aps) # aps enable
Node4 (config-red-aps) # exit
Node4 (config-red) # associate group channel13
Node4 (config-red-aps) # aps working transparent 9/3/0
Node4 (config-red-aps) # aps protection transparent 11/3/0
Node4 (config-red-aps) # aps y-cable
Node4 (config-red-aps) # aps revertive
Node4 (config-red-aps) # aps enable
Node4 (config-red-aps) # end

Node4 # copy system:running-config nvram:startup-config
```

Configuring a Line Card Protected Meshed Ring with Unprotected Channels and OSC

Line card protection requires different shelf and CLI configuration from splitter protection. The following sections describe an example based on the meshed ring topology shown in Figure 10-33 on page 10-63.

Node 1

The configuration for node 1 is the same as described in the “Node 1” section on page 10-73.

Node 2

Figure 10-46 shows the shelf configuration for node 2 in the line card protected meshed ring with unprotected channels shown in Figure 10-33 on page 10-63. Channels 1-4 are line card protected using a nonsplitter line card motherboard in slot 2 and a nonsplitter line card motherboard in slot 4. Slot 8 uses a nonsplitter line card motherboard for the unprotected channels.

Figure 10-46 Shelf Configuration for Node 2 in Line Card Protected Meshed Ring with Unprotected Channels

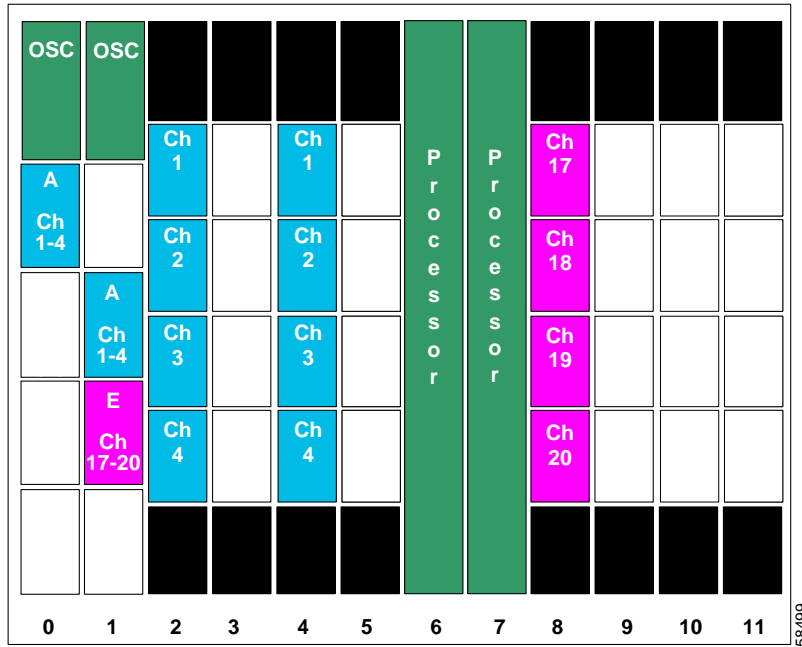
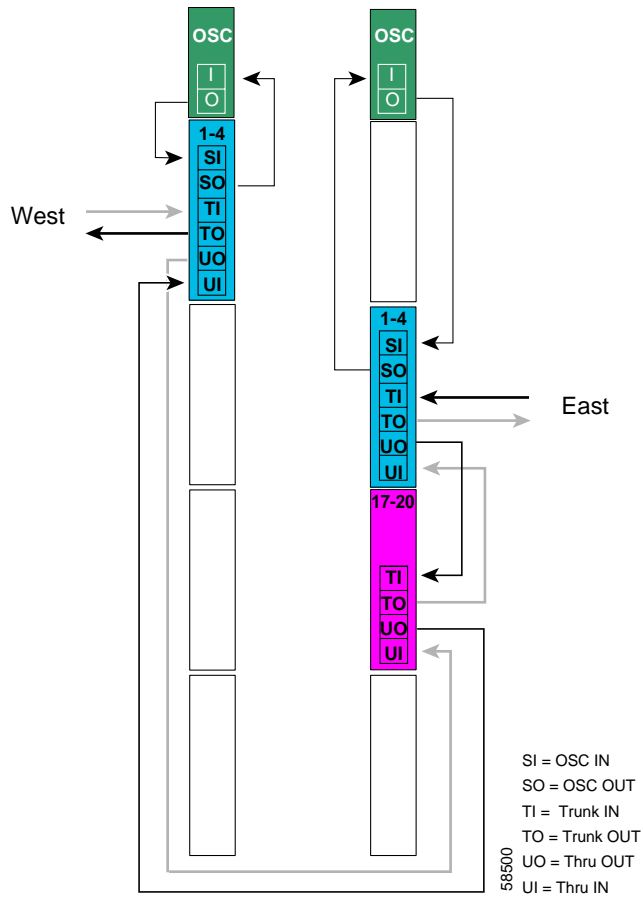


Figure 10-47 shows how the 4-channel mux/demux modules are cabled for node 2 in the line card protected meshed ring with unprotected channels shown in Figure 10-33 on page 10-63.

Figure 10-47 Add/Drop Mux/Demux Module Cabling for Node 2 in Line Card Protected Meshed Ring with Unprotected Channels



Patch Connections

```

Node2# configure terminal
Node2(config)# patch thru 0/0 thru 1/2
Node2(config)# patch wdm 1/2 thru 1/1
Node2(config)# patch wave 0 oscfilter 0/0
Node2(config)# patch wave 1 oscfilter 1/1

Node2(config)# patch wavepatch 2/0/0 filter 0/0/0
Node2(config)# patch wavepatch 2/1/0 filter 0/0/1
Node2(config)# patch wavepatch 2/2/0 filter 0/0/2
Node2(config)# patch wavepatch 2/3/0 filter 0/0/3

Node2(config)# patch wavepatch 4/0/0 filter 1/1/0
Node2(config)# patch wavepatch 4/1/0 filter 1/1/1
Node2(config)# patch wavepatch 4/2/0 filter 1/1/2
Node2(config)# patch wavepatch 4/3/0 filter 1/1/3

Node2(config)# patch wavepatch 8/0/0 filter 1/2/0
  
```

```
Node2(config)# patch wavepatch 8/1/0 filter 1/2/1
Node2(config)# patch wavepatch 8/2/0 filter 1/2/2
Node2(config)# patch wavepatch 8/3/0 filter 1/2/3
```

Transparent Interfaces in Slot 2

```
Node2(config)# interface transparent 2/0/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 2/1/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
Node2(config)# interface wave 2/1
Node2(config-if)# laser frequency 192200
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 2/2/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 2/3/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit
Node2(config)# interface wave 2/3
Node2(config-if)# laser frequency 192400
Node2(config-if)# exit
```

Transparent Interfaces in Slot 4

```
Node2(config)# interface transparent 4/0/0
Node2(config-if)# encapsulation sonet oc12
Node2(config-if)# monitor enable
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 4/1/0
Node2(config-if)# encapsulation sonet oc12
Node2(config-if)# monitor enable
Node2(config-if)# exit
Node2(config)# interface wave 4/1
Node2(config-if)# laser frequency 192200
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 4/2/0
Node2(config-if)# encapsulation sonet oc12
Node2(config-if)# monitor enable
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 4/3/0
Node2(config-if)# encapsulation sonet oc12
Node2(config-if)# monitor enable
Node2(config-if)# exit
Node2(config)# interface wave 4/3
Node2(config-if)# laser frequency 192400
Node2(config-if)# exit
```

Transparent Interfaces in Slot 8

```
Node2(config)# interface transparent 8/0/0
Node2(config-if)# encapsulation sonet oc12
Node2(config-if)# monitor enable
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 8/1/0
Node2(config-if)# encapsulation sonet oc12
Node2(config-if)# monitor enable
Node2(config-if)# exit
Node2(config)# interface wave 8/1
Node2(config-if)# laser frequency 194200
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 8/2/0
Node2(config-if)# encapsulation sonet oc12
Node2(config-if)# monitor enable
Node2(config-if)# exit
```

```
Node2(config)# interface transparent 8/3/0
Node2(config-if)# encapsulation sonet oc12
Node2(config-if)# monitor enable
Node2(config-if)# exit
Node2(config)# interface wave 8/3
Node2(config-if)# laser frequency 194400
Node2(config-if)# exit
```

OSC Interfaces

```
Node2(config)# interface wave 0
Node2(config-if)# no shutdown
Node2(config-if)# exit
```

```
Node2(config)# interface wave 1
Node2(config-if)# no shutdown
Node2(config-if)# exit
```

APS

Use the following for configuring y-cable protection.

```
Node2(config)# redundancy
Node2(config-red)# associate group channel1
Node2(config-red-aps)# aps working transparent 2/0/0
Node2(config-red-aps)# aps protection transparent 4/0/0
Node2(config-red-aps)# aps y-cable
Node2(config-red-aps)# aps revertive
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# exit
Node2(config-red)# associate group channel2
Node2(config-red-aps)# aps working transparent 2/1/0
Node2(config-red-aps)# aps protection transparent 4/1/0
Node2(config-red-aps)# aps y-cable
Node2(config-red-aps)# aps revertive
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# exit
Node2(config-red)# associate group channel3
Node2(config-red-aps)# aps working transparent 2/2/0
```

```

Node2(config-red-aps)# aps protection transparent 4/2/0
Node2(config-red-aps)# aps y-cable
Node2(config-red-aps)# aps revertive
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# exit
Node2(config-red)# associate group channel4
Node2(config-red-aps)# aps working transparent 2/3/0
Node2(config-red-aps)# aps protection transparent 4/3/0
Node2(config-red-aps)# aps y-cable
Node2(config-red-aps)# aps revertive
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# end

Node2# copy system:running-config nvram:startup-config

```

Node 3

Figure 10-48 shows how the modules are installed in the shelf for node 3 in the example network shown in Figure 10-33 on page 10-63. Channels 5–8 are line card protected using a nonsplitter line card motherboard in slot 3 and a nonsplitter line card motherboard in slot 5. Channels 13–16 are line card protected using a nonsplitter line card motherboard in slot 9 and a nonsplitter line card motherboard in slot 11. Slot 8 uses a nonsplitter line card motherboard for the unprotected channels.

Figure 10-48 Shelf Configuration for Node 3 in Line Card Protected Meshed Ring with Unprotected Channels

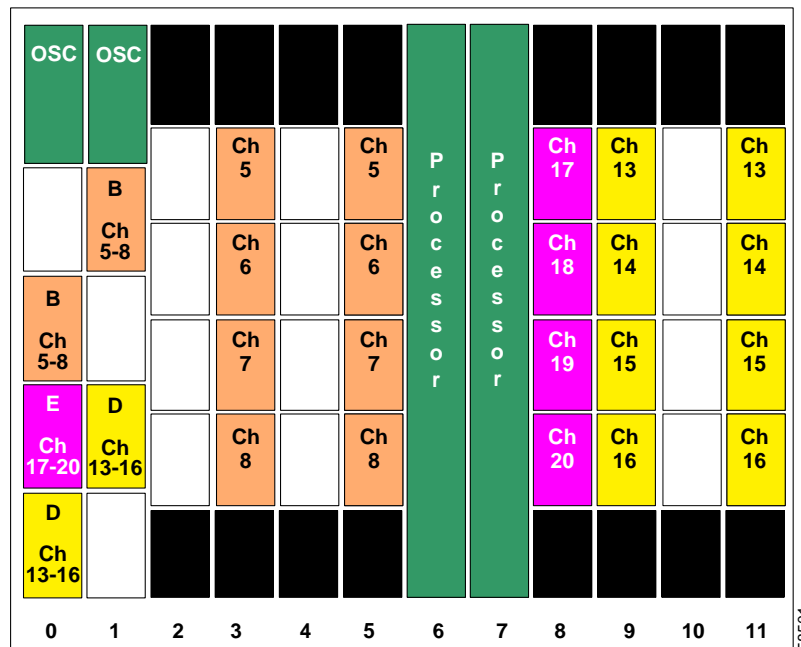
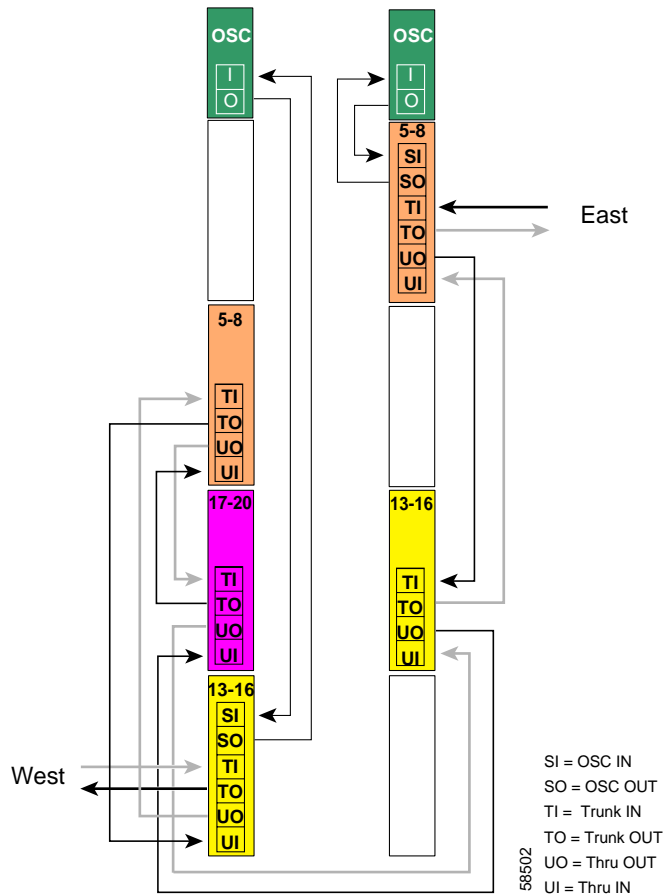


Figure 10-49 shows how the 4-channel mux/demux modules are cabled for node 3 in the line card protected meshed ring with unprotected channels shown in Figure 10-33 on page 10-63.

Figure 10-49 Add/Drop Mux/Demux Module Cabling for Node 3 in Line Card Protected Meshed Ring with Unprotected Channels



Patch Connections

```

Node3# configure terminal
Node3 (config)# patch thru 0/3 wdm 0/1
Node3 (config)# patch thru 0/1 wdm 0/2
Node3 (config)# patch thru 0/2 thru 1/2
Node3 (config)# patch wdm 1/2 thru 1/0
Node3 (config)# patch wave 0 oscfilter 0/3
Node3 (config)# patch wave 1 oscfilter 1/0

Node3 (config)# patch wavepatch 3/0/0 filter 1/0/0
Node3 (config)# patch wavepatch 3/1/0 filter 1/0/1
Node3 (config)# patch wavepatch 3/2/0 filter 1/0/2
Node3 (config)# patch wavepatch 3/3/0 filter 1/0/3

Node3 (config)# patch wavepatch 5/0/0 filter 0/1/0
Node3 (config)# patch wavepatch 5/1/0 filter 0/1/1
Node3 (config)# patch wavepatch 5/2/0 filter 0/1/2
Node3 (config)# patch wavepatch 5/3/0 filter 0/1/3
  
```

```
Node3(config)# patch wavepatch 8/0/0 filter 0/2/0
Node3(config)# patch wavepatch 8/1/0 filter 0/2/1
Node3(config)# patch wavepatch 8/2/0 filter 0/2/2
Node3(config)# patch wavepatch 8/3/0 filter 0/2/3

Node3(config)# patch wavepatch 9/0/0 filter 1/2/0
Node3(config)# patch wavepatch 9/1/0 filter 1/2/1
Node3(config)# patch wavepatch 9/2/0 filter 1/2/2
Node3(config)# patch wavepatch 9/3/0 filter 1/2/3

Node3(config)# patch wavepatch 11/0/0 filter 0/3/0
Node3(config)# patch wavepatch 11/1/0 filter 0/3/1
Node3(config)# patch wavepatch 11/2/0 filter 0/3/2
Node3(config)# patch wavepatch 11/3/0 filter 0/3/3
```

Transparent Interfaces in Slot 3

```
Node3(config)# interface transparent 3/0/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit

Node3(config)# interface transparent 3/1/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
Node3(config)# interface wave 3/1
Node3(config-if)# laser frequency 192700
Node3(config-if)# exit

Node3(config)# interface transparent 3/2/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit

Node3(config)# interface transparent 3/3/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
Node3(config)# interface wave 3/3
Node3(config-if)# laser frequency 192900
Node3(config-if)# exit
```

Transparent Interfaces in Slot 5

```
Node3(config)# interface transparent 5/0/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit

Node3(config)# interface transparent 5/1/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
Node3(config)# interface wave 5/1
Node3(config-if)# laser frequency 192700
Node3(config-if)# exit

Node3(config)# interface transparent 5/2/0
```

```

Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit

Node3 (config)# interface transparent 5/3/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit
Node3 (config)# interface wave 5/3
Node3 (config-if)# laser frequency 192900
Node3 (config-if)# exit

```

Transparent Interfaces in Slot 8

```

Node3 (config)# interface transparent 4/0/0
Node3 (config-if)# encapsulation sonet oc12
Node3 (config-if)# monitor enable
Node3 (config-if)# exit

Node3 (config)# interface transparent 4/1/0
Node3 (config-if)# encapsulation sonet oc12
Node3 (config-if)# monitor enable
Node3 (config-if)# exit
Node3 (config)# interface wave 4/1
Node3 (config-if)# laser frequency 194200
Node3 (config-if)# exit

Node3 (config)# interface transparent 4/2/0
Node3 (config-if)# encapsulation sonet oc12
Node3 (config-if)# monitor enable
Node3 (config-if)# exit

Node3 (config)# interface transparent 4/3/0
Node3 (config-if)# encapsulation sonet oc12
Node3 (config-if)# monitor enable
Node3 (config-if)# exit
Node3 (config)# interface wave 4/3
Node3 (config-if)# laser frequency 194400
Node3 (config-if)# exit

```

Transparent Interfaces in Slot 9

```

Node3 (config)# interface transparent 9/0/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit

Node3 (config)# interface transparent 9/1/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit
Node3 (config)# interface wave 9/1
Node3 (config-if)# laser frequency 1953700
Node3 (config-if)# exit

Node3 (config)# interface transparent 9/2/0
Node3 (config-if)# encapsulation gigabitethernet
Node3 (config-if)# monitor enable
Node3 (config-if)# exit

```



```
Node3(config)# interface transparent 9/3/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
Node3(config)# interface wave 9/3
Node3(config-if)# laser frequency 193900
Node3(config-if)# exit
```

Transparent Interfaces in Slot 11

```
Node3(config)# interface transparent 11/0/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
```

```
Node3(config)# interface transparent 11/1/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
Node3(config)# interface wave 11/1
Node3(config-if)# laser frequency 1953700
Node3(config-if)# exit
```

```
Node3(config)# interface transparent 11/2/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
```

```
Node3(config)# interface transparent 11/3/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit
Node3(config)# interface wave 11/3
Node3(config-if)# laser frequency 193900
Node3(config-if)# exit
```

OSC Interfaces

```
Node3(config)# interface wave 0
Node3(config-if)# no shutdown
Node3(config-if)# exit
```

```
Node3(config)# interface wave 1
Node3(config-if)# no shutdown
Node3(config-if)# exit
```

APS

Use the following for configuring y-cable protection.

```
Node3(config)# redundancy
Node3(config-red)# associate group channel5
Node3(config-red-aps)# aps working transparent 3/0/0
Node3(config-red-aps)# aps protection transparent 5/0/0
Node3(config-red-aps)# aps y-cable
Node3(config-red-aps)# aps revertive
```

```

Node3 (config-red-aps) # aps enable
Node3 (config-red-aps) # exit
Node3 (config-red) # associate group channel6
Node3 (config-red-aps) # aps working transparent 3/1/0
Node3 (config-red-aps) # aps protection transparent 5/1/0
Node3 (config-red-aps) # aps y-cable
Node3 (config-red-aps) # aps revertive
Node3 (config-red-aps) # aps enable
Node3 (config-red-aps) # exit
Node3 (config-red) # associate group channel7
Node3 (config-red-aps) # aps working transparent 3/2/0
Node3 (config-red-aps) # aps protection transparent 5/2/0
Node3 (config-red-aps) # aps y-cable
Node3 (config-red-aps) # aps revertive
Node3 (config-red-aps) # aps enable
Node3 (config-red-aps) # exit
Node3 (config-red) # associate group channel8
Node3 (config-red-aps) # aps working transparent 3/3/0
Node3 (config-red-aps) # aps protection transparent 5/3/0
Node3 (config-red-aps) # aps y-cable
Node3 (config-red-aps) # aps revertive
Node3 (config-red-aps) # aps enable
Node3 (config-red-aps) # exit

Node3 (config-red) # associate group channel13
Node3 (config-red-aps) # aps working transparent 11/0/0
Node3 (config-red-aps) # aps protection transparent 9/0/0
Node3 (config-red-aps) # aps y-cable
Node3 (config-red-aps) # aps revertive
Node3 (config-red-aps) # aps enable
Node3 (config-red-aps) # exit
Node3 (config-red) # associate group channel14
Node3 (config-red-aps) # aps working transparent 11/1/0
Node3 (config-red-aps) # aps protection transparent 9/1/0
Node3 (config-red-aps) # aps y-cable
Node3 (config-red-aps) # aps revertive
Node3 (config-red-aps) # aps enable
Node3 (config-red-aps) # exit
Node3 (config-red) # associate group channel15
Node3 (config-red-aps) # aps working transparent 11/2/0
Node3 (config-red-aps) # aps protection transparent 9/2/0
Node3 (config-red-aps) # aps y-cable
Node3 (config-red-aps) # aps revertive
Node3 (config-red-aps) # aps enable
Node3 (config-red-aps) # exit
Node3 (config-red) # associate group channel16
Node3 (config-red-aps) # aps working transparent 11/3/0
Node3 (config-red-aps) # aps protection transparent 9/3/0
Node3 (config-red-aps) # aps y-cable
Node3 (config-red-aps) # aps revertive
Node3 (config-red-aps) # aps enable

Node3 # copy system:running-config nvram:startup-config

```

Node 4

The configuration for node 4 is the same as described in the “Node 4” section on page 10-89.



Monitoring Your Network Topology

This chapter describes how to configure and manage your network topology. This chapter includes the following sections:

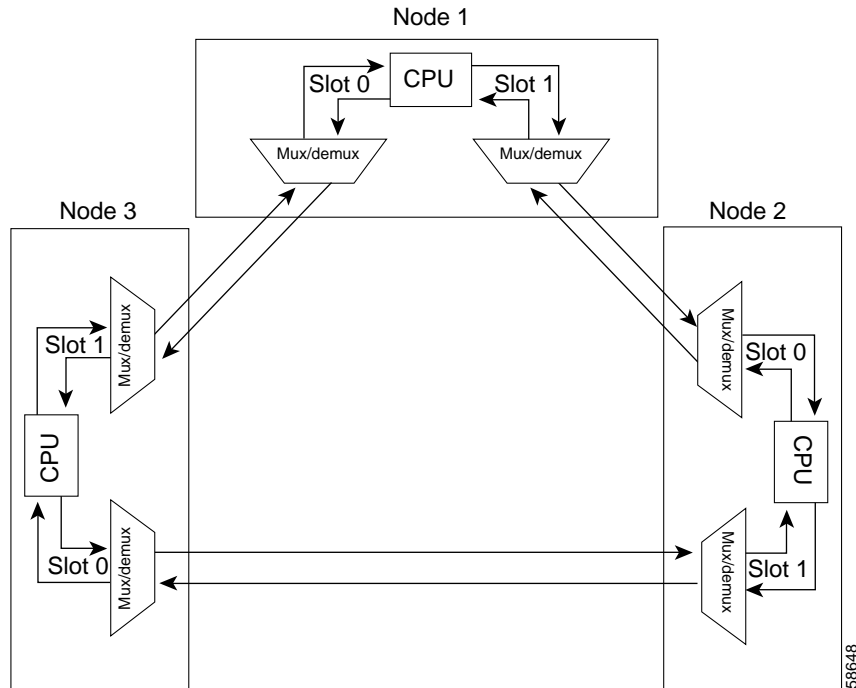
- About the OSC, page 11-1
- Configuring CDP, page 11-3
- Configuring OSCP, page 11-6
- Configuring IP on the OSC, page 11-9
- Configuring SNMP, page 11-14
- Monitoring Without the OSC or In-Band Message Channel, page 11-18
- Configuring Interfaces in the Network Topology, page 11-20
- About Embedded CiscoView, page 11-21
- Installing and Configuring Embedded CiscoView, page 11-21

About the OSC

As described in the “Optical Supervisory Channel” section on page 1-9, the Cisco ONS 15540 ESPx dedicates a separate channel (channel 0) for the OSC (optical supervisory channel), which is used for network control and management information between Cisco ONS 15540 ESPx systems on the network. The OSC is carried on the same fiber as the data channels (channels 1 through 32), but it carries no client data traffic.

Figure 11-1 shows the path of the OSC in a protected ring configuration. The OSC signal is generated by a laser on each mux/demux motherboard and is sent in both directions from the node; both receive signals are monitored to maintain communication with the neighboring nodes. The OSC signal terminates at each node.

Figure 11-1 OSC Signal Path in a Ring Configuration



The OSC performs the following functions:

- **Discovery**—CDP (Cisco Discovery Protocol) sends packets on the OSC to discover neighboring nodes. CDP runs by default every 60 seconds. The information gathered by CDP can be displayed using the CLI (command-line interface) and used by the NMS (network management system) to discover the logical topology of the network.
- **Monitoring**—OSCP (OSC Protocol) runs over the OSC to provide monitoring of the status of adjacent nodes. OSCP is a keepalive mechanism similar to the PNNI Hello protocol used in ATM (Asynchronous Transfer Mode). Using OSCP, nodes exchange packets that allow them to determine the operational status of their neighbors. OSCP must establish that there is two-way communication before declaring to the upper layer protocols that a node is “up.”
- **Management**—IP packets are carried over the OSC to support SNMP and Telnet sessions. Using Telnet over the OSC allows you to access the CLI of all systems on your Cisco ONS 15540 ESPx network with a single Ethernet connection. Also, just one Ethernet connection is required from the NMS to monitor all Cisco ONS 15540 ESPx systems on the network using SNMP.

Hardware Guidelines for Using OSC

The OSC signal is generated using a dedicated laser on the mux/demux motherboards. To provide protection against failure of the laser or a fiber break in protected configurations (point-to-point or ring), the following rules apply:

- Both mux/demux motherboards must support OSC.
- One mux/demux module in each slot must support OSC along with a band of wavelengths.
- The wdm interface of each mux/demux module that supports OSC must connect to the trunk fiber.

For more information on hardware configuration rules, refer to the *Cisco ONS 15540 ESPx Planning Guide*.

Configuring CDP

<<see

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_r/frprt3/frd3001b.htm#1033748

CDP is primarily used to obtain protocol addresses of neighboring devices and to discover the platform of those devices. For a full description of CDP and details on configuring the protocol, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*. For a full description of the CDP commands, refer to the *Cisco IOS Configuration Fundamentals Command Reference*.

On the Cisco ONS 15540 ESPx, you can configure CDP at both the global level and the interface level. The global-level CDP configuration sets the attributes for the entire system. The interface-level configuration identifies interfaces connected to the client equipment and to the trunk interface to CDP. Because there are only optical connections to the client equipment, you must explicitly identify the transparent interfaces connected to the client equipment. On wdm interfaces, you can choose to provide the information about the interface in the CLI or you can let CDP discover it.



Note

The shelf must include the OSC to support CDP. If the OSC is not present, see the “Monitoring Without the OSC or In-Band Message Channel” section on page 11-18.

Configuring Global CDP

To configure CDP on your Cisco ONS 15540 ESPx, use the following commands in global configuration mode:

Command	Purpose
cdp advertise-v2	Specifies CDP version 2 advertisements. The default is version 2.
cdp holdtime <i>seconds</i>	Specifies the amount of time the receiving device should hold a CDP packet from the sending device before discarding it. The default value is 180 seconds.
cdp timer <i>seconds</i>	Specifies how often to send CDP updates. The default value is 60 seconds.
[no] cdp run	Enables and disables CDP on the device. The default state is enabled.

Examples

In the following example, the CDP packets being sent from your device should be held by the receiving device for 60 seconds before being discarded:

```
Switch(config)# cdp holdtime 60
```

In the following example, CDP updates are sent every 80 seconds:

```
Switch(config)# cdp timer 80
```

Displaying the Global CDP Configuration

To display the configured CDP values, use the following EXEC command:

Command	Purpose
show cdp	Displays the configured CDP timer, holdtime, and advertisement settings.

Example

The following example shows how to display the configured CDP values:

```
Switch> show cdp
```

```
Global CDP information:
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 180 seconds
  Sending CDPv2 advertisements is enabled
```

Displaying Global CDP Information

You can display information gathered by CDP, including a specific neighbor device listed in the CDP table, the interfaces on which CDP is enabled, and the traffic between devices gathered using CDP.

To display the CDP information, use the following EXEC commands:

Command	Purpose
show cdp entry {[* <i>entry-name</i>] [protocol version]}	Displays information about all neighbors or a specific neighbor discovered by CDP. Optionally, displays the protocol and version.
show cdp interface [<i>type number</i>]	Displays information about the interfaces on which CDP is enabled.
show cdp neighbors	Displays a list of CDP neighbors.
show cdp traffic	Displays information about traffic between devices gathered using CDP.

Example

The following example shows how to display CDP status and activity information:

```
Switch1# show cdp entry *
-----
Device ID: Switch2
Entry address(es):
  IP address: 10.1.1.2
Platform: cisco , Capabilities: Router
Interface: Wave0, Port ID (outgoing port): Wave0
Holdtime : 176 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) ONS-15540 Software (manopt-I-M), Experimental Version 12.1 [koj-ons 122]
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Mon 30-Apr-01 12:04 by koj
advertisement version: 2

Switch1# show cdp interface
```

```

Wave0 is up, line protocol is up
  Encapsulation UNKNOWN
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds

Switch1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID         Local Intrfce   Holdtme    Capability Platform  Port ID
Switch2           Wave0          158        R           Wave0    Wave0

Switch1# show cdp traffic
CDP counters :
  Total packets output: 18, Input: 20
  Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
  No memory: 0, Invalid packet: 0, Fragmented: 0
  CDP version 1 advertisements output: 0, Input: 0
  CDP version 2 advertisements output: 18, Input: 20

```

Clearing Global CDP Information

You can reset the CDP traffic counters to zero and clear the table that contains the CDP neighbor information. To clear the CDP information, use the following privileged EXEC commands:

Command	Purpose
<code>clear cdp counters</code>	Resets the CDP traffic counters to zero.
<code>clear cdp table</code>	Clears the table that contains the CDP neighbor information.

Configuring CDP Topology Discovery on Wdm and Tengigethernetphy Interfaces

You can enable CDP topology discovery on the wdm interfaces that connect to the trunk fiber and on tengigethernetphy interfaces connected to equipment that supports CDP. CDP then automatically advertises interface information to neighboring nodes.



Note

The Cisco ONS 15540 ESPx enables CDP topology discovery by default on the wdm interfaces connecting to the trunk fiber.

To configure CDP topology discovery on wdm interfaces, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# topology hold-time <i>seconds</i>	Modifies the interval to hold a nonstatic network topology node entry. The default value is 300 seconds.

	Command	Purpose
Step 2	Switch(config)# interface { wdm slot/subcard tengigetheretphy slot/subcard} Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 3	Switch(config-if)# topology neighbor cdp or Switch(config-if)# topology neighbor disable	Enables CDP topology discovery on the interface. The default is enabled. or Disables CDP on the interface.

Examples

The following example shows how to enable CDP topology discover on a wdm interface:

```
Switch(config)# interface wdm 0/0
Switch(config-if)# topology neighbor cdp
```

The following example shows how to disable CDP topology discovery on a wdm interface:

```
Switch(config)# interface wdm 0/0
Switch(config-if)# topology neighbor disable
```

Displaying CDP Information

You can display interface-level information gathered by CDP, including neighboring devices.

To display the CDP information for an interface, use the following EXEC commands:

Command	Purpose
show topology neighbor [detail]	Displays information about the physical network topology neighbors for the node.
show topology	Displays the global physical network topology configuration.

Example

```
Switch# show topology neighbor
Physical Topology:
```

```
Local Port      Neighbor Node      Neighbor Port
-----
Wd0/0          Node1              wdm1/1
Wd0/1          Node2              wdm0/2
Trans8/1/0     Router1            gigabitethernet1/1
```

```
Switch# show topology
Global Physical Topology configuration:
  Maximum Hold Time = 300 secs
  Trap interval = 60 secs
```

Configuring OSCP

The configurable parameters of the OSCP are described in the following sections.

**Note**

The default values are suitable in most cases.

Configuring the Hello Interval Timer

The OSCP sends Hello packets to adjacent nodes at a configured interval. When five packets fail to get a response from the receiving node, that node is declared “down.” By decreasing the interval at which Hello packets are sent, reaction time to a failed node can be lessened. Increasing the interval reduces the amount of Hello packet traffic.

To configure the OSCP Hello timer interval, use the following global configuration command:

Command	Purpose
<code>ospf timer hello interval <i>milliseconds</i></code>	Configures the Hello interval timer in milliseconds. The default value is 3000 milliseconds.

Example

The following example shows how to set the Hello interval to 500 milliseconds:

```
Switch(config)# ospf timer hello interval 500
```

Configuring the Hello Hold-Down Timer

The Hello hold-down timer specifies the interval during which no more than one Hello packet can be sent. If more than one Hello packet is generated during the hold-down period, the extra packets are delayed. Increasing the hold-down timer limits the number of Hello packets triggered in response to Hello packets received from a neighboring node and reduces the likelihood of Hello packets flooding the OSC.

To configure the OSCP Hello hold-down timer, use the following global configuration command:

Command	Purpose
<code>ospf timer hello holddown <i>milliseconds</i></code>	Configures the Hello hold-down timer in milliseconds. The default value is 100 milliseconds.

Example

The following example shows how to set the Hello hold-down timer to 2000 milliseconds:

```
Switch(config)# ospf timer hello holddown 2000
```

Configuring the Inactivity Factor

The OSCP inactivity factor determines whether or not to declare a link down. The inactivity factor is multiplied by the advertised Hello timer interval of the other node to produce the inactivity time interval. If the system does not receive OSCP packets from the other node before the expiration of the inactivity time interval, the link is declared down.

To configure the OSCP inactivity factor, use the following global configuration command:

Command	Purpose
<code>ospf timer inactivity-factor factor</code>	Configures inactivity factor as a multiple of the Hello interval. The default multiplier is 5.

Example

The following example shows how to configure the inactivity factor to 10 times the Hello interval value:

```
Switch(config)# ospf timer inactivity-factor 10
```

Displaying the OSCP Configuration

You can display the OSCP version, node ID, interfaces, and configured protocol parameters. To display the OSCP configuration, use the following EXEC command:

Command	Purpose
<code>show ospf info</code>	Displays the OSCP configuration.

Example

The following example shows the OSCP configuration:

```
Switch(config)# show ospf info
OSPF protocol version 1, Node ID          0001.6447.a240
No. of interfaces 3, No. of neighbors 0
Hello interval 3000 msec, inactivity factor 5,
Hello hold-down 200 msec
Supported OSPF versions:newest 1, oldest 1
```

Displaying OSCP Neighbors

You can display the information for neighboring nodes monitored by the OSCP. To display the OSCP neighbor status for a node, use the following EXEC command:

Command	Purpose
<code>show ospf neighbor</code>	Displays the OSCP neighbor status.

Example

The following example shows the OSCP neighbors for a node:

```
Switch(config)# show ospf neighbor
OSPF Neighbors
Neighbor Node Id:0009.7c1a.cb20   Port list:
  Local Port   Port ID   Rem Port ID   OSPF state
  ~~~~~
Wave7/0       20E0000   20E0000       2way
```

Configuring IP on the OSC

Configuring IP on the OSC allows you to use one Cisco ONS 15540 ESPx node in the network to monitor all the other Cisco ONS 15540 ESPx nodes in the network. The OSC is a point-to-point signal so any IP configuration valid for point-to-point interfaces is usable.

IP addressing on the OSC can be configured two ways:

- An IP address for each OSC wave interface with each address on a separate subnet.
- An unnumbered address for the OSC wave interfaces that reference another numbered interface.

The IP address of the reference interface is used as the IP packet source address. Use a loopback interface as the reference interface because it is always up. Configure IP address for each node in a separate subnet.



Note You can alternatively use the IP address of the NME (network management Ethernet) interface (fastethernet 0) for the reference address instead of the loopback interface.

To configure IP on an OSC wave interface, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface loopback 1 Switch(config-if)#	Selects the loopback interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# ip address ip-address subnet-mask	Configures IP address and subnet for the interface.
Step 3	Switch(config-if)# exit Switch(config)#	Exits interface configuration mode and returns to global configuration mode.
Step 4	Switch(config)# interface fastethernet 0 Switch(config-if)#	Selects the NME interface to configuration and enters interface configuration mode.
Step 5	Switch(config-if)# ip address ip-address subnet-mask	Configures IP address and subnet for the interface.
Step 6	Switch(config-if)# exit Switch(config)#	Exits interface configuration mode and returns to global configuration mode.
Step 7	Switch(config)# interface wave 0 Switch(config-if)#	Selects the wave interface on slot 0.
Step 8	Switch(config-if)# ip unnumbered loopback 1	Configures an unnumbered interface referencing the loopback interface.
Step 9	Switch(config-if)# exit Switch(config)#	Exits interface configuration mode and returns to global configuration mode.
Step 10	Switch(config)# interface wave 1 Switch(config-if)#	Selects the wave interface on slot 1.
Step 11	Switch(config-if)# ip unnumbered loopback 1	Configures an unnumbered interface referencing the loopback interface.

	Command	Purpose
Step 12	Switch(config-if)# exit Switch(config)#	Exits interface configuration mode and returns to global configuration mode.
Step 13	Switch(config)# ip route <i>prefix prefix-mask interface</i> or Switch(config)# router ospf <i>process-id</i> Switch(config-router)# network <i>network-address wildcard-mask area area-id</i> or Switch(config)# router eigrp <i>as-number</i> Switch(config-router)# network <i>network-number [network-mask]</i> or Switch(config)# router bgp <i>as-number</i> Switch(config-router)# network <i>network-number [mask network-mask]</i> Switch(config-router)# neighbor { <i>ip-address peer-group-name</i> } remote-as <i>number</i>	Configures IP static routes for some or all destinations. or Configures OSPF as the routing protocol. or Configures EIGRP as the routing protocol. or Configures BGP as the routing protocol.

**Note**

For detailed information about configuring routing protocols, refer to the *Cisco IOS IP and IP Routing Configuration Guide*.

Example

The following example shows how to configure IP on the OSC on a three node system. Node 1 connects to the NMS (network management system).

```

Node1# configure terminal
Node1(config)# interface loopback 1
Node1(config-if)# ip address 10.1.1.1 255.255.255.0
Node1(config-if)# exit
Node1(config)# interface fastethernet 0
Node1(config-if)# ip address 20.1.1.1 255.255.255.0
Node1(config-if)# exit
Node1(config)# interface wave 0
Node1(config-if)# ip unnumbered loopback 1
Node1(config-if)# exit
Node1(config)# interface wave 1
Node1(config-if)# ip unnumbered loopback 1
Node1(config)# router ospf 1
Node1(config-router)# network 10.1.0.0 0.0.255.255 area 0
Node1(config-router)# network 20.1.0.0 0.0.255.255 area 0

Node2# configure terminal
Node2(config)# interface loopback 1
Node2(config-if)# ip address 10.1.2.2 255.255.255.0
Node2(config-if)# exit
Node2(config)# interface wave 0
Node2(config-if)# ip unnumbered loopback 1

```

```

Node2(config-if)# exit
Node2(config)# interface wave 1
Node2(config-if)# ip unnumbered loopback 1
Node2(config)# router ospf 1
Node2(config-router)# network 10.1.0.0 0.0.255.255 area 0

Node3# configure terminal
Node3(config)# interface loopback 1
Node3(config-if)# ip address 10.1.3.3 255.255.255.0
Node3(config-if)# exit
Node3(config)# interface wave 0
Node3(config-if)# ip unnumbered loopback 1
Node3(config-if)# exit
Node3(config)# interface wave 1
Node3(config-if)# ip unnumbered loopback 1
Node3(config)# router ospf 1
Node3(config-router)# network 10.1.0.0 0.0.255.255 area 0

```

Verifying Connectivity Over the OSC

To verify connectivity over the OSC, use the following EXEC command:

Command	Purpose
<code>telnet ip-address</code>	Connects to another node using the reference IP address for the other node.

Example

The following example shows how to Telnet from node 1 to node 2 in the ring to another through the OSC:

```

Node1# telnet 10.1.2.2
Trying 10.1.2.2 ... Open
Node2> enable
Node2#

```

Configuring IP on Ethernetdcc Interfaces for the In-Band Message Channel

Configuring IP on the in-band message channel allows you to use one Cisco ONS 15540 ESPx node in the network to monitor all the other Cisco ONS 15540 ESPx nodes in the network. The 10-Gbps transponder modules and the 10-GE uplink cards support the in-band message channel.

IP addressing for the in-band message channel can be configured in two ways:

- An IP address for each ethernetdcc interface with each address on a separate subnet.
- An unnumbered address for the Ethernet interfaces that reference another numbered interface.

The IP address of the reference interface is used as the IP packet source address. Use a loopback interface as the reference interface because it is always up. Configure the IP address for each node in a separate subnet. Refer also to the “Interface Naming Conventions” section on page 2-4 for naming conventions.

**Note**

You can alternatively use the IP address of the NME (network management Ethernet) interface (fastethernet 0) for the reference address instead of the loopback interface.

To configure IP on an ethernetdcc interface, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface loopback 1 Switch(config-if)#	Selects the loopback interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# ip address <i>ip-address</i> <i>subnet-mask</i>	Configures IP address and subnet for the interface.
Step 3	Switch(config-if)# exit Switch(config)#	Exits interface configuration mode and returns to global configuration mode.
Step 4	Switch(config)# interface fastethernet 0 Switch(config-if)#	Selects the NME interface to configuration and enters interface configuration mode.
Step 5	Switch(config-if)# ip address <i>ip-address</i> <i>subnet-mask</i>	Configures IP address and subnet for the interface.
Step 6	Switch(config-if)# exit Switch(config)#	Exits interface configuration mode and returns to global configuration mode.
Step 7	Switch(config)# interface ethernetdcc <i>slot/subslot/port</i> Switch(config-if)#	Selects the ethernetdcc interface.
Step 8	Switch(config-if)# ip unnumbered loopback 1	Configures an unnumbered interface referencing the loopback interface.

	Command	Purpose
Step 9	Switch(config-if)# exit Switch(config)#	Exits interface configuration mode and returns to global configuration mode.
Step 10	Switch(config)# ip route <i>prefix prefix-mask interface</i> or Switch(config)# router ospf <i>process-id</i> Switch(config-router)# network <i>network-address wildcard-mask area area-id</i> or Switch(config)# router eigrp <i>as-number</i> Switch(config-router)# network <i>network-number [network-mask]</i> or Switch(config)# router bgp <i>as-number</i> Switch(config-router)# network <i>network-number [mask network-mask]</i> Switch(config-router)# neighbor { <i>ip-address peer-group-name</i> } remote-as <i>number</i>	Configures IP static routes for some or all destinations. or Configures OSPF as the routing protocol. or Configures EIGRP as the routing protocol. or Configures BGP as the routing protocol.

**Note**

For detailed information about configuring routing protocols, refer to the *Cisco IOS IP and IP Routing Configuration Guide*.

Example

The following example shows how to configure IP on the OSC on a three node system. Node 1 connects to the NMS (network management system).

```
Node1# configure terminal
Node1(config)# interface loopback 1
Node1(config-if)# ip address 10.1.1.1 255.255.255.0
Node1(config-if)# exit
Node1(config)# interface fastethernet 0
Node1(config-if)# ip address 20.1.1.1 255.255.255.0
Node1(config-if)# exit
Node1(config)# interface ethernetdcc 4/0/0
Node1(config-if)# ip unnumbered loopback 1
Node1(config-if)# exit
Node1(config)# interface ethernetdcc 4/0/1
Node1(config-if)# ip unnumbered loopback 1
Node1(config-if)# exit
```

Displaying the Ethernetdcc Interface Configuration

To display the ethernetdcc interface configuration, use the following EXEC command:

Command	Purpose
<code>show interfaces ethernetdcc slot/subcard/port</code>	Displays the IP ethernetdcc interface configuration.

Example

The following example shows how to display the IP configuration:

```
Switch# show interfaces ethernetdcc 4/0/0
EthernetDcc10/0/0 is up, line protocol is up
  Hardware is cdl_enabled_port
  Interface is unnumbered. Using address of Loopback1 (10.1.1.1)
  MTU 1492 bytes, BW 500000 Kbit, DLY 0 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation SNAP, loopback not set
  Last input 00:00:02, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    26156 packets input, 1569630 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    22 packets output, 2436 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

Verifying Connectivity over the In-Band Message Channel

To verify connectivity over the in-band message channel, use the following EXEC command:

Command	Purpose
<code>telnet ip-address</code>	Connects to another node using the reference IP address for the other node.

Example

The following example shows how to use Telnet to connect from node 1 to node 2 in the ring to another node through the in-band message channel:

```
Node1# telnet 10.1.2.2
Trying 10.1.2.2 ... Open
Node2> enable
Node2#
```

Configuring SNMP

SNMP is an application-layer protocol that allows an SNMP manager, such as NMS (network management system), and an SNMP agent on the managed device to communicate. You can configure SNMPv1, SNMPv2c, or SNMPv3 on the Cisco ONS 15540 ESPx.

The NME (network management Ethernet) ports on the active processor card, named *fastethernet 0*, provide multiple simultaneous SNMP network management sessions to the current active processor. The Cisco ONS 15540 ESPx can be fully managed by sending SNMP messages to the active processor IP address. If a processor switchover occurs, you can access the other processor card after it reaches the active state. For more information on processor card redundancy, see the “About Processor Card Redundancy” section on page 3-15.

**Note**

The standby processor card does not respond to SNMP messages.

For detailed instructions on configuring SNMP and enabling SNMP trap notifications, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* and the *Cisco IOS Configuration Fundamentals Command Reference* publication.

Enabling MIB Notifications

The Cisco ONS 15540 ESPx supports SMNP trap notifications through MIBs. This section describes the following MIBs:

- Alarm threshold MIB
- APS MIB
- OSCP MIB
- Patch MIB
- Redundancy facility MIB
- Physical topology MIB

You can find the complete list of MIBs supported on the Cisco ONS 15540 ESPx and the MIB module definition files on the Cisco MIB website on Cisco.com. For more information on accessing the MIBs module definition files, refer to the *MIBs Quick Reference for the Cisco ONS 15500 Series*.

Alarm Threshold MIB

The interface alarm threshold MIB (CISCO-IF-THRESHOLD-MIB) assists SNMP monitoring of the interface alarm threshold activity. To enable the SNMP trap notifications for alarm threshold activity, use the following global configuration command:

Command	Purpose
<code>snmp-server enable traps threshold min-severity {degrade failure}</code>	Enables SNMP trap notifications for alarm threshold activity.

For information about other commands that enable SNMP trap notifications, refer to the *Cisco IOS Configuration Fundamentals Command Reference* publication.

Example

The following example shows how to enable SNMP trap notifications for alarm thresholds and set the minimum notification severity to signal degrade.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps threshold min-severity degrade
```

APS MIB

The APS MIB (CISCO-APS-MIB) assists SNMP monitoring of SONET APS activity. To enable the SNMP trap notifications for APS activity between associated interfaces, use the following global configuration command:

Command	Purpose
snmp-server enable traps aps	Enables SNMP trap notifications for APS activity.

For information about other commands that enable SNMP trap notifications, refer to the *Cisco IOS Configuration Fundamentals Command Reference* publication.

Example

The following example shows how to enable SNMP trap notifications for APS.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps aps
```

OSCP MIB

The OSCP MIB (CISCO-OSCP-MIB) assists SNMP monitoring of OSCP activity. To enable the SNMP trap notifications for OSCP activity, use the following global configuration command:

Command	Purpose
snmp-server enable traps oscp	Enables SNMP trap notifications for OSCP activity.

For information about other commands that enable SNMP trap notifications, refer to the *Cisco IOS Configuration Fundamentals Command Reference* publication.

Example

The following example shows how to enable SNMP trap notifications for OSCP.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps oscp
```

Patch MIB

The patch MIB (CISCO-OPTICAL-PATCH-MIB) assists SNMP monitoring of patch connections. To enable the SNMP trap notifications for patch connection creation, modification, and deletion, use the following global configuration command.

Command	Purpose
snmp-server enable traps patch	Enables SNMP trap notifications for patch connection activity.

For information about other commands that enable SNMP trap notifications, refer to the *Cisco IOS Configuration Fundamentals Command Reference* publication.

Example

The following example shows how to enable SNMP trap notifications for patch connections:

```
Switch# configure terminal
Switch(config)# snmp-server enable traps patch
```

Physical Topology MIB

The network physical topology MIB (PTOPO-MIB) assists SNMP monitoring of network topology activity. To enable the SNMP trap notifications for network topology activity, use the following global configuration command.

Command	Purpose
snmp-server enable traps topology [throttle-interval seconds]	Enables SNMP trap notifications for network topology activity.

For information about other commands that enable SNMP trap notifications, refer to the *Cisco IOS Configuration Fundamentals Command Reference* publication.

Example

The following example shows how to enable SNMP trap notifications for network topology activity:

```
Switch# configure terminal
Switch(config)# snmp-server enable traps topology
```

Redundancy Facility MIB

The redundancy facility MIB (CISCO-RF-MIB) assists SNMP monitoring of processor redundancy activity. To enable the SNMP trap notifications for processor redundancy activity, use the following global configuration command.

Command	Purpose
snmp-server enable traps rf	Enables SNMP trap notifications for the redundancy facility activity.

For information about other commands that enable SNMP trap notifications, refer to the *Cisco IOS Configuration Fundamentals Command Reference* publication.

Example

The following example shows how to enable SNMP trap notifications for processor redundancy activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps rf
```

Monitoring Without the OSC or In-Band Message Channel

To take advantage of the OSC, the Cisco ONS 15540 ESPx system must be equipped with one mux/demux module with OSC (for unprotected configurations) or two mux/demux modules with OSC (for protected configurations). To take advantage of the in-band message channel, the system must be equipped with in-band message channel capable interfaces. If your system is not equipped to support the OSC or in-band message channel, the following conditions apply:

- You cannot reach other nodes on the network using Telnet or SNMP. Separate connections to each system must exist on the network for management purposes.
- CDP does not function on the network. The physical topology must be configured manually for fault isolation and system management.
- Keepalive information is not available for other nodes on the network.

Setting Up Connections to Individual Nodes

To access individual nodes in a Cisco ONS 15540 ESPx network without the OSC, you must establish separate connections to a management port on each system. This can be done using a Telnet session over an Ethernet connection, a console connection, or a modem connection to the auxiliary port. For instructions on how to do this, see Chapter 3, “Initial Configuration.”

For NMS without the OSC, each node reports individually to the NMS. Thus you must connect the NMS to each node using SNMP over an Ethernet connection. [Refer to NMS documentation](#)

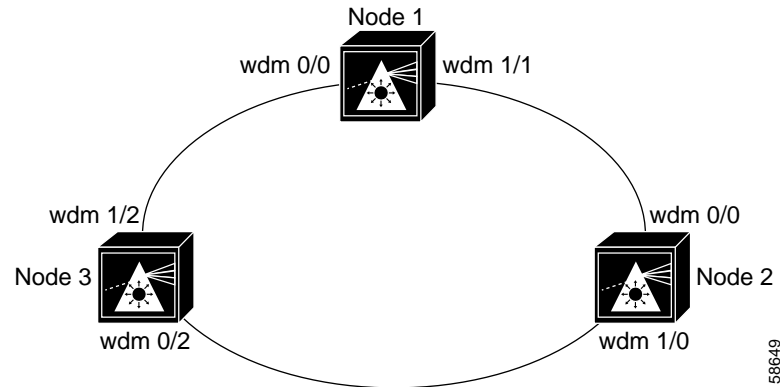
Manually Configuring the Network Topology

If the OSC or in-band message channel is absent from the system or CDP is disabled, you must manually add the wdm and tengigethernetphy interfaces connected to the trunk fiber to the network topology using the CLI. To manually add the wdm interfaces to the network topology, perform the following steps on all the nodes in the network, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface wdm { wdm slot/subcard tengigethernetphy slot/subcard } Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# topology neighbor { name node-name ip-address node-ip-address mac-address node-mac-address } { port { name port-name ip-address port-ip-address mac-address port-mac-address }}	Configures the network topology information for a neighboring node.
Step 3	Switch(config-if)# topology neighbor agent ip-address ip-address	Specifies the address of the network topology agent on a neighboring node.

Figure 11-2 shows an example ring topology with three shelves.

Figure 11-2 Ring Topology Example



Examples

The following example shows how to configure the network topology for node 1 in Figure 11-2:

```

Node1(config)# interface wdm 1/1
Node1(config-if)# topology neighbor name Node2 port name wdm0/0
Node1(config-if)# topology neighbor agent ip-address 10.2.2.2
Node1(config)# exit
Node1(config)# interface wdm 0/0
Node1(config-if)# topology neighbor name Node3 port name wdm1/2
Node1(config-if)# topology neighbor agent ip-address 10.3.3.3
  
```

The following example shows how to configure the network topology for node 2 in Figure 11-2:

```

Node2(config)# interface wdm 0/0
Node2(config-if)# topology neighbor name Node1 port name wdm1/1
Node2(config-if)# topology neighbor agent ip-address 10.1.1.1
Node2(config)# exit
Node2(config)# interface wdm 1/0
Node2(config-if)# topology neighbor name Node3 port name wdm0/2
Node2(config-if)# topology neighbor agent ip-address 10.3.3.3
  
```

The following example shows how to configure the network topology for node 3 in Figure 11-2:

```

Node3(config)# interface wdm 0/2
Node3(config-if)# topology neighbor name Node2 port name wdm1/0
Node3(config-if)# topology neighbor agent ip-address 10.2.2.2
Node3(config)# exit
Node3(config)# interface wdm 1/2
Node3(config-if)# topology neighbor name Node1 port name wdm0/0
Node3(config-if)# topology neighbor agent ip-address 10.1.1.1
  
```

Displaying the Network Topology

To display the network topology, use the following EXEC command:

Command	Purpose
<code>show topology neighbor</code>	Displays the network topology.

Example

The following example shows the network topology:

```
Switch# show topology neighbor

Physical Topology:

Local Port      Neighbor Node      Neighbor Port
-----
Wd0/0           Node1              wdm1/1
Wd0/1           Node2              wdm0/2
```

Configuring Interfaces in the Network Topology

Not all interfaces on the Cisco ONS 15540 ESPx supports CDP topology discovery, such as the transparent and wdm-split interfaces. Also, not all equipment connected to a Cisco ONS 15540 ESPx, such as EDFAs (erbium-doped fiber amplifiers) connected to wdm interfaces, support CDP. In these cases, you must explicitly add the interfaces to the network topology.

To manually add an interface to the network topology, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface { transparent <i>slot/subcard0</i> wdm <i>slot/subcard</i> wdm-split <i>slot/subcard</i> } Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# topology neighbor { name <i>node-name</i> ip-address <i>node-ip-address</i> mac-address <i>node-mac-address</i> } { port { name <i>port-name</i> ip-address <i>port-ip-address</i> mac-address <i>port-mac-address</i> }}	Configures the network topology information for a neighboring node.
Step 3	Switch(config-if)# topology neighbor agent ip-address <i>ip-address</i>	Specifies the address of the network topology agent on a neighboring node.



Note If you manually add an interface to the topology, be sure to manually add the corresponding interface on the neighboring node.

Example

The following example shows how to add a transparent interface to the network topology:

```
Switch(config)# interface transparent 8/1/0
Switch(config-if)# topology neighbor name router1 port name gigabitethernet1/1
Switch(config-if)# topology neighbor agent ip-address 10.1.1.1
```

Displaying Topology Information

To display the topology information, use the following EXEC command:

Command	Purpose
<code>show topology neighbor</code>	Displays network topology information.

Example

The following example shows how to display the client equipment topology:

```
Switch# show topology neighbor
```

```
Physical Topology:
```

```
Local Port      Neighbor Node      Neighbor Port
-----
Trans8/1/0     Router1            gigabitethernet1/1
```

About Embedded CiscoView

The Embedded CiscoView network management system provides a web-based interface for the Cisco ONS 15540 ESPx. Embedded CiscoView uses HTTP and SNMP to provide graphical representations of the system and to provide GUI-based management and configuration facilities. After you install and configure Embedded CiscoView, you can access your Cisco ONS 15540 ESPx from a web browser utility.

You can download the Embedded CiscoView files from the following URL:

<http://www.cisco.com/kobayashi/sw-center/netmgmt/ciscoview/embed-cview-planner.shtml>

Installing and Configuring Embedded CiscoView

To install and configure Embedded CiscoView on the Cisco ONS 15540 ESPx, perform the following steps:

	Command	Purpose
Step 1	Switch# <code>dir {bootflash: slotn: diskn:}</code>	Displays the contents of the specified Flash memory device, including the amount of free space that is available. If enough free space is available, skip to Step 4
Step 2	Switch# <code>delete {bootflash:filename slotn:filename diskn:filename}</code>	Deletes an old file to make room for the new file.
Step 3	Switch# <code>squeeze {bootflash: slotn:}</code>	Recovers the space on the Flash memory device.
Step 4	Switch# <code>copy tftp: {bootflash: slotn: diskn:}</code>	Copies the CiscoView tar file (ONS15540-1.tar) from the TFTP server. If you are installing Embedded CiscoView for the first time, skip to Step 7.
Step 5	Switch# <code>delete {bootflash:cv/* slotn:cv/* diskn:cv/*}</code>	Removes existing files from the CiscoView directory.

	Command	Purpose
Step 6	Switch# squeeze { bootflash: slotn: diskn: }	Recovers the space in the file system.
Step 7	Switch# archive tar /xtract bootflash:ONS15540-1.tar bootflash:cv or Switch# archive tar /xtract slotn:ONS15540-1.tar slotn:cv or Switch# archive tar /xtract diskn:ONS15540-1.tar diskn:cv	Extracts the CiscoView files from the tar file on the TFTP server to the CiscoView directory.
Step 8	Switch# dir { bootflash: slotn: diskn: }	Displays the file in Flash memory. Repeat Step 1 and Step 8 for the file system on the standby processor (sby-bootflash: , sby-diskn: or sby-slotn:).
Step 9	Switch# configure terminal Switch(config)#	Enters global configuration mode.
Step 10	Switch(config)# ip http server	Enables the HTTP web server.
Step 11	Switch(config)# end Switch#	Returns to privileged EXEC mode.
Step 12	Switch# copy system:running-config nvram:startup-config	Saves the configuration in NVRAM.

Examples

The following example shows how to initially install Embedded CiscoView on both processors in your system:

```
Switch# copy tftp slot0:
Address or name of remote host []? 20.1.1.1
Source filename []? ONS15540-1.tar
Destination filename [ONS15540-1.tar]?
Accessing tftp://20.1.1.1/ONS15540-1.tar...
Loading ONS15540-1.tar from 20.1.1.1 (via Port-channel1.1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1251840/2503680 bytes]

1251840 bytes copied in 109.848 secs (11484 bytes/sec)

Switch# archive tar /xtract slot0:ONS15540-1.tar slot0:/cv
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC

8510CSR# dir slot0:
Directory of slot0:/

   1  -rw-     2276396  Apr 30 2001 17:48:07  ONS15540-i-mz.121
   2  -rw-     1251840  May 23 2001 14:03:35  ONS15540-1.tar
   3  -rw-         8861  May 23 2001 14:26:05  cv/ONS15540-1.0.html
   4  -rw-    1183238  May 23 2001 14:26:06  cv/ONS15540-1.0.sgz
   5  -rw-         3704  May 23 2001 14:27:55  cv/ONS15540-1.0_ace.html
   6  -rw-          401  May 23 2001 14:27:55  cv/ONS15540-1.0_error.html
   7  -rw-        17003  May 23 2001 14:27:55  cv/ONS15540-1.0_jks.jar
```



```

 8 -rw-      17497   May 23 2001 14:27:57 cv/ONS15540-1.0_nos.jar
 9 -rw-      8861   May 23 2001 14:27:59 cv/applet.html
10 -rw-       529   May 23 2001 14:28:00 cv/cisco.x509
11 -rw-      2523   May 23 2001 14:28:00 cv/identitydb.obj

```

16384000 bytes total (1287752 bytes free)

```

Switch# copy tftp: sby-slot0:ONS15540-1.tar
Address or name of remote host []? 20.1.1.1
Source filename []? ONS15540-1.tar
Destination filename [ONS15540-1.tar]?
Accessing tftp://20.1.1.1/ONS15540-1.tar...
Loading ONS15540-1.tar from 20.1.1.1 (via Port-channel1.1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1251840/2503680 bytes]

```

1251840 bytes copied in 109.848 secs (11484 bytes/sec)

```

Switch# archive tar /xtract slot0:ONS15540-1.tar sby-slot0:cv
cccccccccccccccccccccccccccccccccccccccccccccccccccccccc

```

```

Switch# dir sby-slot0:
Directory of sby-slot0:/

```

```

 1 -rw-      2276396   May 20 2001 17:48:07 ONS15540-i-mz.121
 2 -rw-      1251840   May 23 2001 14:03:35 ONS15540-1.tar
 3 -rw-       8861    May 23 2001 14:26:05 cv/ONS15540-1.0.html
 4 -rw-     1183238   May 23 2001 14:26:06 cv/ONS15540-1.0.sgz
 5 -rw-       3704    May 23 2001 14:27:55 cv/ONS15540-1.0_ace.html
 6 -rw-       401    May 23 2001 14:27:55 cv/ONS15540-1.0_error.html
 7 -rw-      17003    May 23 2001 14:27:55 cv/ONS15540-1.0_jks.jar
 8 -rw-      17497    May 23 2001 14:27:57 cv/ONS15540-1.0_nos.jar
 9 -rw-      8861    May 23 2001 14:27:59 cv/applet.html
10 -rw-       529    May 23 2001 14:28:00 cv/cisco.x509
11 -rw-      2523    May 23 2001 14:28:00 cv/identitydb.obj

```

16384000 bytes total (1287752 bytes free)

```

Switch# configure terminal
Switch(config)# ip http server
Switch(config)# end
Switch# copy system:running-config nvram:startup-config

```

The following example shows how to update the CiscoView files on your Cisco ONS 15540 ESPx:

```

Switch# delete slot0:cv/*
Delete filename [cv/*]?
Delete slot0:cv/ONS15540-1.0.html? [confirm]
Delete slot0:cv/ONS15540-1.0.sgz? [confirm]
Delete slot0:cv/ONS15540-1.0_ace.html? [confirm]
Delete slot0:cv/ONS15540-1.0_error.html? [confirm]
Delete slot0:cv/ONS15540-1.0_jks.jar? [confirm]
Delete slot0:cv/ONS15540-1.0_nos.jar? [confirm]
Delete slot0:cv/applet.html? [confirm]
Delete slot0:cv/cisco.x509? [confirm]
Delete slot0:cv/identitydb.obj? [confirm]

Switch# squeeze slot0:
All deleted files will be removed. Continue? [confirm]
Squeeze operation may take a while. Continue? [confirm]

```

Squeeze of slot0 complete

```

Switch# copy tftp slot0:
Address or name of remote host []? 20.1.1.1
Source filename []? ONS15540-1.tar
Destination filename [ONS15540-1.tar]?

```

```

Accessing tftp://20.1.1.1/ONS15540-1.tar...
Loading ONS15540-1.tar from 20.1.1.1 (via Port-channel1.1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1251840/2503680 bytes]

1251840 bytes copied in 109.848 secs (11484 bytes/sec)

Switch# archive tar /xtract slot0:ONS15540-1.tar slot0:cv
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC

Switch# delete sby-slot0:cv/*
Delete filename [cv/*]?
Delete slot0:cv/ONS15540-1.0.html? [confirm]
Delete slot0:cv/ONS15540-1.0.sgz? [confirm]
Delete slot0:cv/ONS15540-1.0_ace.html? [confirm]
Delete slot0:cv/ONS15540-1.0_error.html? [confirm]
Delete slot0:cv/ONS15540-1.0_jks.jar? [confirm]
Delete slot0:cv/ONS15540-1.0_nos.jar? [confirm]
Delete slot0:cv/applet.html? [confirm]
Delete slot0:cv/cisco.x509? [confirm]
Delete slot0:cv/identitydb.obj? [confirm]
Switch# squeeze sby-lot0:
All deleted files will be removed. Continue? [confirm]
Squeeze operation may take a while. Continue? [confirm]
Squeeze of sby-slot0 complete
Switch# copy tftp sby-lot0:
Address or name of remote host [20.1.1.1]?
Source filename [ONS15540-1.tar]?
Destination filename [ONS15540-1.tar]?
Accessing tftp://20.1.1.1/ONS15540-1.tar...
Loading ONS15540-1.tar from 20.1.1.1 (via Port-channel1.1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1251840/2503680 bytes]

1251840 bytes copied in 109.848 secs (11484 bytes/sec)
Switch# archive tar /xtract slot0:ONS15540-1.tar slot0:cv
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Switch# archive tar /xtract tftp://10.1.1.1/ciscoview.tar sby-slot0:cv

```

Accessing Embedded CiscoView

Access Embedded CiscoView using the NME IP address as the URL for your Cisco ONS 15540 ESPx from a web browser using the following format:

http://A.B.C.D/

Displaying Embedded CiscoView Information

To display the Embedded CiscoView information, use the following EXEC commands:

Command	Purpose
show ciscoview package	Displays information about the Embedded CiscoView files in the Flash PC Card.
show ciscoview version	Displays the Embedded CiscoView version.

Example

The following example shows how to display the Embedded CiscoView file and version information:

```
Switch# show ciscoview package
File source:flash:
CVFILE                               SIZE(in bytes)
-----
ONS15540-1.0.html                    8861
ONS15540-1.0.sgz                     1183238
ONS15540-1.0_ace.html                3704
ONS15540-1.0_error.html              401
ONS15540-1.0_jks.jar                 17003
ONS15540-1.0_nos.jar                 17497
applet.html                           8861
cisco.x509                             529
identitydb.obj                        2523

Switch# show ciscoview version
Engine Version: 5.3 ADP Device: ONS15540 ADP Version: 1.0 ADK: 39
```




Numerics

- 10-Gbps line card motherboards
 - description **1-3**
- 10-GE transponder modules
 - configuration overview **5-1**
 - description **1-3, 1-8**
- 2.5-Gbps line card motherboards
 - description **1-3**
- 2.5-Gbps transponder modules
 - configuration overview **4-1**
 - description **1-3**

A

- AAA
 - configuring **3-8**
- add/drop mux/demux modules
 - description **1-3**
 - interfaces **2-8, 2-9**
 - See also mux/demux modules
- aggregate shelf Ethernet interfaces. See ASE interfaces
- alarm threshold
 - rates (table) **4-11, 5-9**
- alarm thresholds
 - configuring **4-9, 5-7**
 - description **4-9, 5-7**
 - displaying configuration **4-12, 5-10**
 - MIBs **11-15**
 - rates (table) **4-10, 5-8**
- ALS
 - laser safety control and **4-15**
- amplifiers. See EDFAs

APS

- configuring dual shelf nodes **8-5 to 8-7**
- configuring line card protection **7-8 to 7-10**
- configuring splitter protection **7-2 to 7-6**
- lockouts **7-30 to 7-33**
- MIBs **11-16**
- switchovers **7-30 to 7-33**
- aps clear command **7-32**
- aps direction command **7-19**
- aps disable command **7-4, 7-9, 7-15, 7-19, 8-6**
- aps enable command **6-3, 7-4, 7-9, 7-14, 7-15, 7-19, 7-24, 7-26, 7-27, 7-29, 8-6**
- aps far-end command **8-6**
- aps lockout command **7-31**
- APS lockouts. See lockouts
- aps message-channel command **6-3, 7-14**
- aps protection command **6-3, 7-4, 7-9, 7-14, 8-6**
- aps revertive command **7-15**
- aps switch command **7-31**
- APS switchovers. See switchovers
- aps timer message holddown command **7-29**
- aps timer message max-interval command **7-29**
- aps timer oscp holddown command **7-19**
- aps timer oscp max-interval command **7-19**
- aps timer search-for-up command **7-24, 7-26, 7-27**
- aps timer wait-to-restore command **7-15**
- aps trigger command **4-10, 5-8**
- aps working command **6-3, 7-4, 7-9, 7-14, 7-19, 8-6**
- aps y-cable command **7-9, 8-6**
- ASE interfaces
 - not supported (note) **2-10**
- associate group command **6-3, 7-4, 7-9, 7-14, 7-15, 7-19, 8-6**
- associate interface command **7-4**

Authentication, Authorization, and Accounting. See AAA

autoboot

configuring **3-20**

displaying configuration **3-20**

See also booting

automatic laser shutdown. See ALS

Automatic Protection Switching. See APS

automatic synchronization

causes (table) **3-22**

configuring **3-21**

auto-sync running-config command **3-22**

auto-sync startup-config command **3-22**

auxiliary ports

interface naming convention **2-10**

modem support **3-2**

B

bands

description **1-3**

bidirectional path switching

configuring **7-19**

description **7-18**

displaying configuration **7-23**

example (figure) **7-20**

figure **7-18**

boot command **3-33**

booting

default behavior **3-32**

bootload failure

system response **3-32**

boot system command **3-20, 3-32**

Break key

controlling **3-31**

C

CDL

configuring IP **11-11 to 11-14**

cdl enable command **5-3**

CDP

clearing information **11-5**

configuring **11-3 to 11-6**

description **11-3**

displaying configuration **11-4**

displaying information **11-4**

cdp advertise-v2 command **11-3**

cdp holdtime command **11-3**

cdp run command **11-3**

cdp timer command **11-3**

channel bands. See bands

channels

description **1-3**

OSC **1-9**

See also data channels

Cisco Discovery Protocol. See CDP

Cisco ONS 15540

configuration overview **2-10**

starting up **3-2**

See also hardware; shelf; software

CiscoView. See Embedded CiscoView

CiscoWorks2000

support **1-9**

clear cdp counters command **11-5**

clear cdp table command **11-5**

clear performance history command **4-26, 5-19**

CLI

description **2-1**

help **2-3**

client equipment

monitoring **11-20**

client protection

configuring **7-6, 7-7**

description **7-6, 7-7**

See also line card protection; y-cable protection

client signals

extended range transponder support **1-5**

- MM transponder support 1-5
- SM transponder support 1-4
- transparent interfaces and 2-6
- clock rate command 4-3
- clock rates
 - configuring 4-2 to 4-5
 - displaying configuration 4-6
 - laser shutdown and (note) 4-5
- command, disconnect ssh 3-12
- command, ip domain-name 3-11
- command, show ip ssh 3-12
- command, ssh 3-12
- command hostname 3-11
- command-line interface. See CLI
- command modes
 - description 2-1
 - table 2-2
- commands
 - abbreviating 2-3
 - listing 2-3
- command show ssh 3-12
- compliance 1-8
- components
 - description 1-3 to 1-8
- config-register command 3-20, 3-33
- configuration register
 - changing value 3-20
 - See software configuration register
- configurations
 - displaying 3-6
 - overview of tasks 2-10
 - synchronizing 3-21 to 3-22
- connectivity
 - checking 3-14
- console ports
 - configuring modem support 3-2
 - using 3-2
 - See also NME
- conventions

- naming interfaces 2-4 to 2-10
- CPU. See processor cards
- critical temperature shutdown
 - configuring 3-37
 - description 3-36
 - displaying thresholds 3-37
- cross connect drawers
 - description 1-4
- cross connections
 - description 4-24, 5-16
 - displaying 4-25, 5-17
- crypto key command 3-11

D

- data channels
 - OSC and 1-10, 11-1
 - transponder module support 1-4
- description command 4-10, 5-8
- diagnostic tests. See online diagnostics
- digital video. See DV
- disconnect ssh command 3-12
- documentation
 - related xx
- dual shelf nodes
 - configuring 8-1 to 8-7
 - description 8-1
- duplex command 3-4
- DV
 - support on transponder modules 4-5

E

- Embedded CiscoView
 - accessing 11-24
 - description 11-21
 - download URL 11-21
 - installing 11-21 to 11-25

enable password command **3-4**

enable passwords
description **3-3**

enable secret command **3-4**

enable secret passwords
description **3-3**

encapsulation. See protocol encapsulation

encapsulation command **4-3**

Enterprise Systems Connection. See ESCON

environment-monitor shutdown fan command **3-35**

environment-monitor shutdown temperature
command **3-37**

environment-monitor temperature-threshold
command **3-37**

erbium-doped fiber amplifiers. See EDFAs

ESCON
configuring protocol encapsulation (table) **4-3**
configuring protocol monitoring **1-7, 4-6**
network topologies and (note) **10-1**

ethernetdcc interfaces **11-11**

Ethernet management ports. See NME

extended range transponder modules
description **1-5**

F

fan failure shutdown
configuring **3-35**
description **3-34**
displaying configuration **3-35**

Fast Ethernet
configuring protocol encapsulation (table) **4-3**

fastethernet 0 interfaces
configuring **3-3 to 3-6**
configuring IP addresses **3-4**
description **2-9**
IP on in-band message channel **11-12**
IP on OSC **11-9**
See also NME

fastethernet-sby 0 interfaces
description **2-9**
See also NME

FDDI
configuring protocol encapsulation (table) **4-3**

Fiber Connection. See FICON

Fibre Channel
configuring protocol encapsulation (table) **4-3**
configuring protocol monitoring **1-7, 4-6**

FICON
configuring protocol encapsulation (table) **4-3**
configuring protocol monitoring **1-7, 4-6**

filter interfaces
description **2-8**

firewalls
configuring **3-14**

Flash PC Cards
displaying contents **11-21**

forward laser control
configuring **4-16**
configuring tengigethernetphy interfaces **5-11**
configuring waveethernetphy interfaces **5-11**
description **4-13**
displaying configuration **4-17, 5-12**
figure **4-13**
OFC and (caution) **4-16**

G

Gigabit Ethernet
configuring protocol encapsulation (table) **4-3**
configuring protocol monitoring **1-7, 4-6**

H

hardware
components **1-3 to 1-8**
features **1-1 to 1-8**

- OSC guidelines **11-2**
- shelf overview **1-1**
- Hello hold-down timer
 - configuring **11-7**
- Hello inactivity factor
 - configuring **11-7**
- Hello interval timer
 - configuring **11-7**
- help
 - CLI **2-3**
- hostname command **3-6, 3-11**
- host names
 - configuring **3-6**
- hubbed ring topologies
 - configuring line card protection **10-22 to 10-45**
 - configuring splitter protection **10-3 to 10-21**
 - description **10-1**
 - example (figure) **10-2**

I

- in-band message channel
 - description **1-9**
 - displaying configuration **5-4, 11-14**
 - enabling on tengigethernetphy interfaces **5-3**
 - verifying connectivity **11-14**
- interface ethernetdcc command **11-12**
- interface loopback command **11-9, 11-12**
- interfaces
 - line card protection model (figure) **2-6**
 - naming conventions **2-4 to 2-10**
 - splitter protection model (figure) **2-5**
 - See also specific types of interfaces (for example, filter interfaces)
- interface tengigethernetphy command **5-11**
- interface transparent command **4-3**
- interface wave command **4-16, 4-17, 4-20, 5-14, 6-8, 6-9, 11-9**
- interface waveethernetphy command **5-11**
- interface wavepatch command **7-11**

- interface wdm command **11-18**
- IP
 - configuring on OSC interfaces **11-9 to 11-11**
 - configuring over CDL **11-11 to 11-14**
- ip address command **3-4, 11-9, 11-12**
- IP addresses
 - configuring on NME **3-4**
 - ethernetdcc interfaces **11-11**
 - OSC wave interfaces **11-9**
- ip default-gateway command **3-4**
- ip domain-name command **3-11**
- ip route command **11-10, 11-13**
- ip unnumbered command **11-9, 11-12**

K

- Kerberos
 - configuring **3-9**

L

- laser control. See forward laser control; laser safety control
- laser control forward enable command **4-16, 5-11**
- laser control safety enable command **4-17**
- lasers
 - displaying status **5-16**
 - turning on and off **5-15**
- laser safety control
 - configuring **4-17**
 - description **4-15**
 - displaying configuration **4-18**
 - figure **4-15**
 - line card protection and **4-17**
 - OFC and (caution) **4-17**
 - splitter protection and (caution) **4-15, 7-4**
- laser shutdown
 - configuring **4-16 to 4-18**
 - description **4-13 to 4-15**

laser shutdown command **5-15**

line card motherboards

- configuring for line card protection **7-11**
- displaying cross connections (example) **4-25, 5-17**
- splitter protection and **7-3, 7-8**
- wavepatch interfaces **2-7**

line card protection

- configuring dual shelf topologies **8-1 to 8-7**
- configuring hubbed ring topologies **10-22 to 10-45**
- configuring meshed ring topologies **10-72 to 10-94**
- configuring point-to-point topologies **9-9 to 9-17**
- configuring splitter protected line card motherboards **7-11**
- configuring y-cable protection **7-8**
- considerations **7-8**
- description **7-6**
- displaying cross connections (example) **4-25, 5-17**
- example (figure) **7-7**
- interface model (figure) **2-6**
- lockouts **7-30 to 7-33**
- switchovers **7-30 to 7-33**
- See also y-cable protection

line card redundancy controllers. See LRCs

line vty command **3-4**

lockouts

- clearing **7-32**
- description **7-30**
- displaying status **7-31, 7-32**
- requesting **7-31**

logical mesh topologies. See meshed ring topologies

loopback command **5-6**

loopbacks

- configuring **5-5 to 5-7**
- displaying configuration **5-6**

LRCs

- description **1-8**

M

maintenance-mode command **3-23**

management ports. See NME

management systems. See network management systems

meshed ring topologies

- configuring line card protection **10-72 to 10-94**
- configuring line card protection with unprotected channels **10-94 to 10-104**
- configuring splitter protection **10-46 to 10-63**
- configuring splitter protection with unprotected channels **10-63 to 10-72**
- description **10-2**
- example (figure) **10-3**

MIBs

- enabling **11-16 to 11-17**
- processor support **3-1**
- supported **11-15**

MM transponder modules

- description **1-5**

modem

- support **3-2**

monitor enable command **4-8**

monitoring. See network monitoring; protocol monitoring

multimode transponder modules. See MM transponder modules

multiple trunk

- support **1-10**

mux/demux cabling

- dual shelf nodes **8-2 to 8-4**
- hubbed ring topologies with line card protection, example **10-23, 10-31, 10-35, 10-39, 10-43**
- hubbed ring topologies with splitter protection, example **10-5, 10-11, 10-14, 10-17, 10-20**
- meshed ring topologies with line card protection, example **10-74, 10-81, 10-85, 10-90**
- meshed ring topologies with splitter protection, example **10-48, 10-53, 10-56, 10-60**
- meshed ring topologies with unprotected channels, line card protection, example **10-96, 10-100**

- meshed ring topologies with unprotected channels, splitter protection, example **10-65, 10-69**
- point-to-point topologies without protection, example **9-19**
- mux/demux modules
 - configuring for line card protection **7-8**
 - interfaces **2-8**
- mux/demux motherboards
 - description **1-3**

N

- network management Ethernet. See NME
- network management systems
 - supported **1-9**
 - See also Embedded CiscoView
- network monitoring
 - CDP **11-3 to 11-5**
 - Embedded CiscoView **11-21 to 11-25**
 - OSCP **11-6 to 11-8**
 - transparent interfaces **11-20**
 - without OSC **11-18 to 11-20**
- Network Time Protocol. See NTP
- network topologies
 - adding interfaces **11-20**
 - configuring neighbor discovery **11-5**
 - MIBs **11-16, 11-17**
 - types **1-10**
 - See also hubbed ring topologies; meshed ring topologies; point-to-point topologies
- NME
 - configuring interfaces **3-3**
 - description **2-9**
 - displaying configuration **3-5**
 - using **3-2**
 - See also fastethernet 0 interfaces
- no environment-monitor temperature-threshold command **3-37**
- notification-throttle timer command **4-9, 5-7**
- NTP
 - configuring **3-7**
 - description **3-6**
 - displaying configuration **3-8**
 - ntp server command **3-7**
 - ntp update-calendar command **3-7**

O

- OADM. See add/drop mux/demux modules
- OFC
 - configuring with encapsulation command **4-3**
 - description **4-14**
 - figure **4-14**
 - forward laser control and (caution) **4-16**
 - laser safety control and (caution) **4-17**
- online diagnostics
 - description **1-10**
- open fiber control. See OFC
- optical add/drop mux/demux modules. See add/drop mux/demux modules
- optical budgets. See optical power budgets
- optical connections. See cross connections
- optical mux/demux motherboards. See mux/demux motherboards
- optical power budgets
 - system specifications **1-8**
- optical power thresholds
 - configuring **4-19, 5-14, 6-8**
 - displaying configuration **4-20, 5-14, 6-9**
 - trunk fiber based protection switchovers **6-4 to 6-8**
- optical supervisory channel. See OSC
- Optical Supervisory Channel Protocol. See OSCP
- optical terminal mux/demux modules. See terminal mux/demux modules
- optical threshold power receive command **4-20, 5-14, 6-8, 6-9**
- OSC
 - description **1-9, 11-1 to 11-2**
 - hardware guidelines **11-2**
 - OSCP **11-6 to 11-8**

- signal path (figure) 11-2
 - oscfiler interfaces
 - configuring patch connections 4-21
 - description 2-9
 - OSC interfaces
 - configuring CDP 11-3 to 11-5
 - configuring IP 11-9 to 11-11
 - description 2-9
 - patch connections 4-21
 - OSCP
 - configuring 11-6 to 11-8
 - description 11-2
 - displaying configuration 11-8
 - displaying neighbors 11-8
 - MIBs 11-16
 - OSC Protocol. See OSCP
 - oscp timer hello holddown command 11-7
 - oscp timer hello interval command 11-7
 - oscp timer inactivity-factor command 11-8
-
- P**
- passwords
 - description 3-3
 - patch command 4-21
 - patch connections
 - configuring 4-2, 4-21 to 4-24, 5-12 to 5-13
 - configuring for PSMs 6-10 to 6-11
 - description 4-21
 - displaying configuration 4-23, 5-13, 6-10
 - types (table) 4-21
 - path lockouts. See lockouts
 - path switching
 - configuring 7-19 to 7-24
 - description 7-17 to 7-19
 - example (figure) 7-17
 - y-cable protection and 7-21 to 7-23
 - path switchovers. See switchovers
 - performance history counters
 - description 4-25, 5-17
 - displaying 4-26, 5-18
 - point-to-point topologies
 - configuring line card protection 9-9 to 9-17
 - configuring splitter protection 9-3
 - configuring without protection 9-17 to 9-21
 - description 9-1
 - example without protection (figure) 9-2
 - example with protection (figure) 9-2
 - multiple trunk support 1-10, 9-3
 - power budgets. See optical power budgets
 - processor cards
 - autoboot 3-20
 - configuring 3-18 to 3-25
 - description 1-8, 3-1
 - hardware state transitions 3-15
 - interfaces 2-9
 - redundant 3-18
 - reloading 3-25
 - slot assignments 1-2
 - software state transitions 3-16
 - starting up 3-2
 - processor redundancy. See redundancy
 - processors. See processor cards
 - processor switchovers
 - forcing 3-18 to 3-19
 - protection
 - description 7-1
 - types 7-2 to 7-10
 - protection switching. See path switching
 - protection switch modules. See PSMs
 - protocol encapsulation
 - configuring 4-2 to 4-5
 - displaying configuration 4-6
 - types supported 1-4
 - protocol monitoring
 - configuring 4-8
 - description 4-6
 - displaying configuration 4-8

PSMs

- configuring interfaces **6-2**
- description **1-3**
- network topology **6-11**
- optical power thresholds **6-4 to 6-9**
- trunk fiber based protection **6-3**

Q

quick laser shutdown. See forward laser control; laser safety control

R

RADIUS

- configuring **3-9**

redundancy

- configuring **3-18 to 3-25**
- description **3-15 to 3-17**
- displaying alarm status (note) **3-15**
- displaying configuration **3-23**
- forcing switchovers **3-18 to 3-19**

MIBS **11-17**

- processor hardware state transitions **3-15**
- processor software state transitions **3-16**
- synchronizing configurations **3-21**

redundancy command **3-22, 7-4**

redundancy manual-sync command **3-21**

redundancy reload peer command **3-25**

redundancy reload shelf command **3-25**

redundancy switch-activity command **3-18**

reset command **3-19**

reshape, retime, retransmit functions. See 3R functions

revertive switching

- configuring **7-15**
- description **7-15**
- displaying configuration **7-16**

ring topologies

- description **10-1 to 10-3**

multiple trunk support **1-10, 10-3**

See also hubbed ring topologies; meshed ring topologies

router bgp command **11-10, 11-13**

router eigrp command **11-10, 11-13**

router ospf command **11-10, 11-13**

S

SDH

configuring protocol encapsulation (table) **4-3**

configuring protocol monitoring **1-7, 4-6**

Secure Shell. See SSH

Secure Shell. See SSH.

security features

- AAA **3-8**
- firewalls **3-14**
- Kerberos **3-9**
- overview **3-8**
- passwords and privileges **3-14**
- RADIUS **3-9**
- TACACS+ **3-10**
- traffic filters **3-14**

selectable transceivers. See transceivers

SFP optics

description **1-5**

shelf

configuration examples

hubbed ring topologies with splitter protection **10-10, 10-16**

point-to-point topologies with line card protection, 32 channels **8-3**

point-to-point topologies without protection **9-18**

configuration overview **2-10**

description **1-1**

layout (figure) **1-2**

starting up **3-2**

show aps command **6-4, 7-5, 7-10, 7-14**

show bootvar command **3-20**

show cdp command **11-4**

- show cdp entry command 11-4
- show cdp interface command 11-4
- show cdp neighbor command 11-4
- show cdp traffic command 11-4
- show ciscoview package command 11-24
- show ciscoview version command 11-24
- show connect command 4-25, 5-17
- show environment command 3-14, 3-35, 3-37
- show flash command 11-21
- show hardware command 3-4
- show interfaces transparent command 4-6
- show ip ssh command 3-12
- show ntp status command 3-8
- show oscp info command 11-8
- show oscp neighbor command 11-8
- show patch command 4-23, 5-13, 6-10
- show performance command 4-26, 5-18
- show processes command 3-13
- show protocols command 3-13
- show redundancy capability command 3-23
- show redundancy running-config-file command 3-23
- show redundancy summary command 3-23, 3-26
- show ssh command 3-12
- show stacks command 3-13
- show threshold-list command 4-12, 5-10
- show topology command 6-12, 11-6, 11-21
- show topology neighbor command 11-19
- show version command 3-20
- shutdown command 4-5, 7-11
- Simple Network Management Protocol. See SNMP
- single-mode transponder modules. See SM transponder modules
- SM transponder modules
 - description 1-4
- SNMP
 - configuring 11-14
 - configuring alarm thresholds (table) 4-9, 5-7
 - processor support 3-1
- snmp-server enable traps aps command 11-16
- snmp-server enable traps oscp command 11-16
- snmp-server enable traps patch command 11-16
- snmp-server enable traps rf command 11-17
- snmp-server enable traps threshold min-severity command 11-15
- snmp-server enable traps topology command 11-17
- software
 - features 1-8 to 1-10
- software configuration register
 - boot field values 3-32
 - Break key, controlling 3-31
 - changing 3-33
 - description 3-30
 - IP broadcast address 3-31
 - response to bootload failure 3-32
 - settings 3-30
 - verifying value 3-34
- SONET
 - configuring protocol encapsulation (table) 4-3
 - configuring protocol monitoring 1-7, 4-6
- SONET APS. See APS
- speed command 3-4
- splitter protection
 - configuring 7-3
 - configuring hubbed ring topologies 10-3 to 10-21
 - configuring meshed ring topologies 10-46 to 10-63
 - configuring meshed ring topologies with unprotected channels 10-63 to 10-72
 - configuring point-to-point topologies 9-3
 - considerations 7-3
 - description 7-2
 - displaying configuration 7-5
 - displaying cross connections (example) 4-25, 5-17
 - example (figure) 7-2
 - figure 2-5
 - interface model (figure) 2-5
 - lockouts 7-30 to 7-33
 - switchovers 7-30 to 7-33
- SRCs

- description 1-8
 - SSH
 - configuring 3-11 to 3-12
 - disconnecting 3-12
 - displaying 3-12
 - overview 3-11
 - ssh command 3-12
 - standards compliance. See compliance
 - standby privilege-mode enable command 3-25
 - standby processor card
 - enabling privileged EXEC mode access 3-25
 - switchcard redundancy controllers. See SRCs
 - switchover command 3-18
 - switchover-enable timer
 - configuring 7-24, 7-25, 7-27, 7-28
 - displaying configuration 7-25, 7-26, 7-28, 7-29
 - switchovers
 - clearing 7-32
 - description 7-30
 - displaying status 7-31, 7-32
 - requesting 7-31
 - types 7-30
 - synchronizing
 - configurations 3-21 to 3-22
 - Synchronous Digital Hierarchy. See SDH
 - system management
 - checking basic connectivity 3-14
 - TACACS 3-10
-
- T**
- TACACS 3-10
 - TACACS+
 - configuring 3-10
 - telnet command 11-11, 11-14
 - tengigethernetphy interfaces
 - configuration overview 5-1
 - configuring alarm thresholds 5-7 to 5-10
 - configuring CDP 11-5
 - configuring forward laser control 5-11
 - description 2-6
 - enabling 5-2
 - loopbacks 5-5 to 5-7
 - terminal mux/demux modules
 - description 1-3
 - See also mux/demux modules
 - threshold command 4-10, 5-8
 - threshold-group command 4-10, 5-8
 - threshold-list command 4-9, 5-7
 - thresholds. See alarm thresholds
 - thru interfaces
 - configuring patch connections 4-21
 - description 2-8
 - topologies. See network topologies
 - topology hold-time command 11-5
 - topology neighbor agent ip-address command 6-11, 6-12, 8-5, 11-18, 11-20
 - topology neighbor cdp command 11-6
 - topology neighbor command 6-11, 6-12, 8-5, 11-18, 11-20
 - topology neighbor disable command 11-6
 - traffic filters
 - configuring 3-14
 - transceivers. See SFP optics
 - transparent interfaces
 - adding to network topology 11-20
 - configuration overview 4-1
 - configuring alarm thresholds 4-9 to 4-13
 - configuring clock rates 4-2 to 4-5
 - configuring protocol encapsulation 4-2 to 4-5
 - configuring protocol monitoring 4-6
 - description 2-6
 - displaying network topology information 6-12, 11-21
 - transponder modules
 - configuring y-cable protection 7-8
 - description 1-4
 - interfaces 2-6, 2-7
 - shutting down lasers 4-13 to 4-18
 - splitter protection and 7-3

y-cable protection and **7-7**

troubleshooting

- cross connections **4-24, 5-16**
- online diagnostics **1-10**
- shelf misconfigurations **4-23, 5-13**

trunk fiber based protection

- configuring wdmsplit interfaces **6-3**
- switchovers and optical power thresholds **6-4 to 6-8**

trunk fiber protection

- considerations **7-13**
- description **7-12**
- scheme (figure) **7-13**

U

unidirectional path switching

- configuring **7-19**
- description **7-17**
- displaying configuration **7-23**
- example (figure) **7-18**

unprotected channels

- configuring in meshed ring topologies **10-63 to 10-72, 10-94 to 10-104**
- configuring in point-to-point topologies **9-17 to 9-21**

V

value command **4-10, 5-8**

W

waveethernetphy interfaces

- configuration overview **5-2**
- configuring alarm thresholds **5-7 to 5-10**
- configuring forward laser control **5-11**
- description **2-7**
- enabling **5-4**
- loopbacks **5-5 to 5-7**

wave interfaces

configuration overview **4-2**

configuring alarm thresholds **4-9 to 4-13**

configuring forward laser control **4-16**

configuring laser safety control **4-17**

configuring patch connections **4-21**

description **2-7**

protocol monitoring **4-7**

wavepassthru interfaces

- configuring patch connections **5-12**

wavepatch interfaces

- configuration overview **5-2**
- configuring patch connections **5-12**
- description **2-7**

wdm interfaces

- adding manually to network topologies, example **11-18 to 11-20**
- configuring CDP **11-5**
- configuring patch connections **4-21**
- description **2-8**
- displaying CDP information **11-6**

wdmrelay interfaces

- configuring patch connections **6-10**

wdmsplit interface

- enabling **6-2**

wdmsplit interfaces

- displaying information **6-2**

Y

y-cable protection

- displaying configuration **7-10**
- path switching and **7-21 to 7-23**