Cisco ONS 15540 ESP 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-9661-01

Cisco ONS 15540 ESP Configuration Guide

CONTENTS

FIGURES

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 ESP 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 ESP.

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 ESP transponder module interfaces.	The performance history counters feature is supported on the Cisco ONS 15540 ESP transponder module interfaces.	"About Performance History Counters" section on page 4-23 "Displaying Performance History Counters" section on page 4-24
SSHv2 support on Cisco ONS 15540 ESP.	The Cisco ONS 15540 ESP 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 ESP.	The Cisco ONS 15540 ESP 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 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 ESP.	This Cisco ONS 15540 ESP supports SNMPv3.	"Configuring SNMP" section on page 9-11

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.	"Transponder Modules" section on page 1-3 "Configuring Protocol Encapsulation or Clock Rate" section on page 4-2 "About Protocol Monitoring" section on page 4-6

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 1-3
Change to s**how 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 ESP Configuration Guide is organized into the following chapters:

- Chapter 1, "Product Overview,"provides an overview of the Cisco ONS 15540 ESP features and functions.
- Chapter 2, "Before You Begin," provides basic information about the Cisco ONS 15540 ESP CLI, IOS mode and naming conventions.
- Chapter 3, "Initial Configuration," describes how to perform the initial configuration of the Cisco ONS 15540 ESP.
- 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 Splitter Protection and Line Card Protection with APS," describes how to configure signal protection on Cisco ONS 15540 ESP systems and networks.
- Chapter 6, "Configuring Dual Shelf Nodes," describes how to configure a network node with two Cisco ONS 15540 ESP shelves supporting 32 channels with line card protection.
- Chapter 7, "Configuring Point-to-Point Topologies," describes how to configure point-to-point network topologies with examples.
- Chapter 8, "Configuring Ring Topologies," describes how to configure ring network topologies with examples.
- Chapter 9, "Monitoring the Network Topology," describes how to monitor the operation of Cisco ONS 15540 ESP networks.

Related Documentation

Use this Cisco ONS 15540 ESP 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 ESP Planning Guide*

  Provides detailed information on the Cisco ONS 15540 ESP architecture and functionality.
- *Cisco ONS 15540 ESP Hardware Installation Guide*

Provides detailed information about installing the Cisco ONS 15540 ESP.

- *Cisco ONS 15540 ESP Optical Transport Turn-Up and Test Guide*

  Provides acceptance testing procedures for Cisco ONS 15540 ESP nodes and networks.
- *Cisco ONS 15540 ESP Command Reference*

  Provides commands to configure and manage the Cisco ONS 15540 ESP.
- *Cisco ONS 15540 ESP System Alarms and Error Messages*

  Describes the system alarms and error messages for the Cisco ONS 15540 ESP.
- *Cisco ONS 15540 ESP Troubleshooting Guide*

  Describes how to identify and resolve problems with the Cisco ONS 15540 ESP.
- *Network Management for the Cisco ONS 15540 ESP*

  Provides information on the network management systems that support the Cisco ONS 15540 ESP.
- *Cisco ONS 15540 ESP TL1 Command Reference*

  Provides a full TL1 command and autonomous message set including parameters, AIDs, conditions and modifiers for the Cisco ONS 15540 ESP.
- *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 ESP Software Upgrade Guide*

  Describes how to upgrade system images and functional images on the Cisco ONS 15540 ESP.
- *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.
italic	Command input that is supplied by the user.
[ ]	Keywords or arguments that appear within square brackets are optional.
{ x | x | x }	A choice of keywords (represented by x) appears in braces separated by vertical bars. The user must select one.
Ctrl	The control key. For example, where Ctrl + D is written, hold down the Control key while pressing the D key.

Convention	Application
`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 ESP (Extended Services Platform) is an optical transport platform that employs DWDM (dense wavelength division multiplexing) technology. With the Cisco ONS 15540 ESP, 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 ESP Planning and Design Guide*.

This chapter includes the following sections:

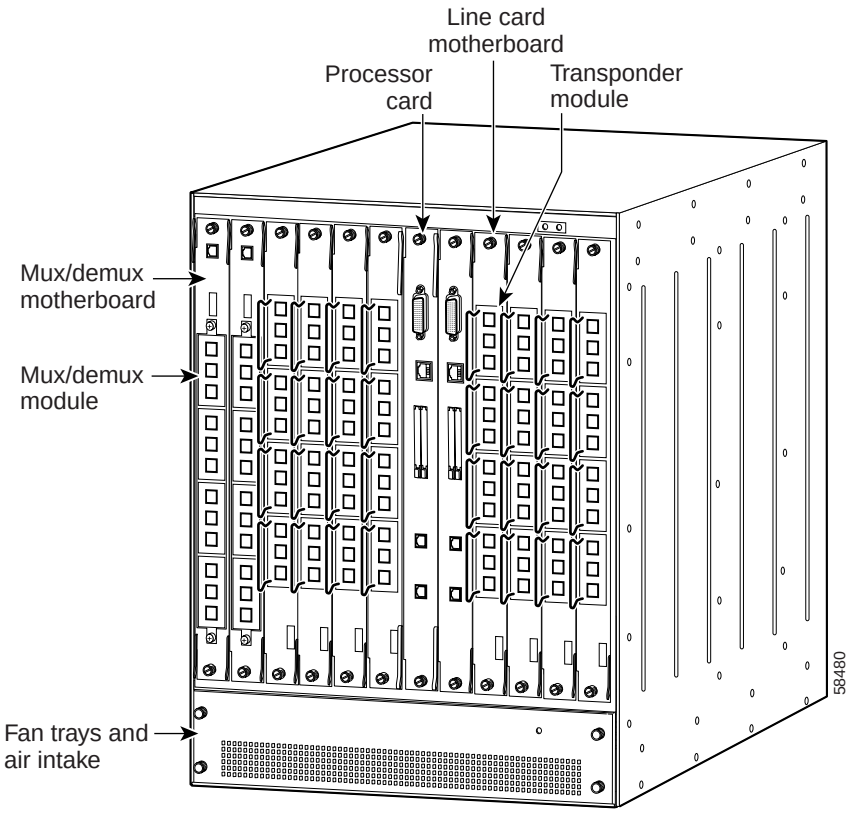
Cisco ONS 15540 ESP Hardware Features

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

Chassis Overview

The Cisco ONS 15540 ESP 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 optical backplane for carrying signals between the transponder modules and the mux/demux modules, and an electrical backplane for system control.

Figure 1-1 Cisco ONS 15540 ESP Shelf Layout



Component Summary

The Cisco ONS 15540 ESP 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. The 2.5-Gbps line card motherboards are modular and can be populated according to user needs.There are three types of 2.5-Gbps line card motherboards: splitter protected, unprotected “west” direction, and unprotected “east” direction.
- 2.5-Gbps transponder modules—Up to four per line card motherboard. Each 2.5-Gbps transponder module has a single external interface to the client side and an internal interface that connects over the system’s optical backplane to the mux/demux modules. The 2.5-Gbps transponder modules are hot pluggable, permitting in-service upgrades and replacement. The 2.5-Gbps transponder modules transmit the ITU wavelength, or channel, to the mux/demux modules.
- Optical mux/demux motherboards—One per system for unprotected operation or two per system for protection. Each mux/demux motherboard can accept up to four mux/demux modules. The mux/demux motherboards are modular and can be populated according to user needs.
- Optical add/drop mux/demux modules—Up to four per mux/demux motherboard. Each add/drop mux/demux module can multiplex and demultiplex a band of 4 or 8 channels, for a maximum of 32 channels. Channels not filtered by the OADM module are passed on to the next add/drop mux/demux module. The add/drop mux/demux modules connect to the trunk side and to the transponder modules over the optical backplane.

- Optical terminal mux/demux modules—Up to two per mux/demux motherboard. Each terminal mux/demux module can multiplex and demultiplex a band of 16 channels, for a maximum of 32 channels. All of the channels received by the terminal mux/demux modules are terminated, none are passed through. The terminal mux/demux modules connect to the trunk side and to the transponder modules over the optical backplane.
- Processor cards—Two per system for fault tolerance. The processor cards provide system processing, redundancy arbitration, clocking, and other central functions.

Transponder Modules

In the transponder module, the client signal is converted into an ITU-compliant wavelength, which is cross-connected over the optical backplane 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 ESP 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

SM Transponder Modules

SM transponder modules have a fixed, non-pluggable transceiver 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.

On the trunk side, the SM transponder modules have output (laser) power in the range of 4 to 8 dBm and receive (detector) sensitivity of –28 dBm. For more information on power budget planning, refer to the *Cisco ONS 15540 ESP Planning Guide*. For power budget specifications for individual components, refer to the *Cisco ONS 15540 ESP Hardware Installation Guide*.

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

- ESCON (Enterprise Systems 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 (1Gbps 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

- ISC (Intersystem Channel Links) compatibility mode

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 FC, ISC compatibility mode, and FICON.

MM Transponder Modules

MM transponder modules have a fixed, non-pluggable transceiver 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.

On the trunk side, the MM transponder modules have output (laser) power in the range of 4 to 8 dBm and receive (detector) sensitivity of –28 dBm. For more information on power budget planning, refer to the *Cisco ONS 15540 ESP Planning Guide*. For power budget specifications for individual components, refer to the *Cisco ONS 15540 ESP Hardware Installation Guide*.

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

- ESCON (Enterprise Systems Connection) (200 Mbps) SM and MM
- SDH (Synchronous Digital Hierarchy) 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
- Sysplex ETR (external timer reference) MM

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

On the trunk side, the Type 2 extended range transponder modules have output (laser) power in the range of 5 to 10 dBm and receive (detector) sensitivity of –28 dBm. For more information on power budget planning, refer to the *Cisco ONS 15540 ESP Planning Guide*. For power budget specifications for individual components, refer to the *Cisco ONS 15540 ESP Hardware Installation Guide*.

Fixed rate SFP optics 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 µm MM 62.5/125 µm	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 µm MM 62.5/125 µm	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 µm MM 62.5/125 µm	850 nm	LC
15500-XVRA-03B1	Gigabit Ethernet[4], Fibre Channel (1 Gbps)[5], FICON (1 Gbps), ISC compatibility mode (1 Gbps), ISC-3 (1 Gbps),	SM 9/125 µm	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 µm	1310 nm	LC
15500-XVRA-06B1	SONET OC-12 SR[8], SDH STM-4	SM 9/125 µm	1310 nm	LC
15500-XVRA-07B1	SONET OC-48 SR, SDH STM-16	SM 9/125 µm	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 µm 62.5/125 µm	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 µm	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 µm 62.5/125 µm	1310 nm	LC
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 2^{23-1}
4. 8B/10B coded

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

- ESCON (Enterprise Systems Connection)
- Fibre Channel (1 Gbps only)
- FICON (Fiber Connection) (1 Gbps only)
- Gigabit Ethernet
- SDH (Synchronous Digital Hierarchy) (STM-1, STM-4, STM-16)

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

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

Mux/Demux Modules

The optical mux/demux modules multiplex signals received over the optical backplane from the transponder modules. The optical mux/demux modules also demultiplex the received signals from the trunk side.

Processor Cards

The Cisco ONS 15540 ESP includes two processor cards for redundancy, one in active mode and the other in hot-standby mode. Each processor card is comprised of 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 (switchcard 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.

Standards Compliance

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

Cisco ONS 15540 ESP Software Feature Overview

The Cisco ONS 15540 ESP 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.
- 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 ESP 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.

Network Management Systems

The Cisco ONS 15540 ESP is supported by the network management system CiscoWorks2000, which includes the following:

- CiscoView
- DFM (Device Fault Manager)
- CTM (Cisco Transport Manager)

For Embedded CiscoView configuration information, see the "Installing and Configuring Embedded CiscoView" section on page 9-19.

For more information on the network management systems that support the Cisco ONS 15540 ESP, refer to the *Network Management for the Cisco ONS 15540 ESP* document.

Optical Supervisory Channel

The Cisco ONS 15540 ESP 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 ESP 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 ESP 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 ESP networks, see Chapter 9, "Monitoring the Network Topology."

Online Diagnostics

The Cisco ONS 15540 ESP 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

For more information on using the online diagnostics, refer to the *Cisco ONS 15540 ESP Troubleshooting Guide*.

Network Topologies

The Cisco ONS 15540 ESP 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 ESP Planning and Design Guide*. Also, for information about configuring network topologies, see Chapter 7, “Configuring Point-to-Point Topologies” and Chapter 9, “Monitoring the Network Topology.”

CHAPTER 2

Before You Begin

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

About the CLI

You can configure the Cisco ONS 15540 ESP 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 ESP 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 via 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 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 **config 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 ESP has two types of motherboards, the 2.5-Gbps line card 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 through the backplane to a mux/demux module in a mux/demux motherboard. The external interfaces of each mux/demux module connects to a pair of fibers, one for the receive direction and one for the transmit direction. The Cisco ONS 15540 ESP CLI supports the following interface types:

- Transparent interfaces
- Wave interfaces
- Wavepatch interfaces
- Wavepassthru interfaces
- Filter interfaces
- Wdm interfaces
- Thru interfaces
- Filterband interfaces
- Filtergroup interfaces
- OSC (optical supervisory channel) interfaces
- NME (network management Ethernet) interfaces

Figure 2-1 shows the interface relationships for splitter protected 2.5-Gbps line card motherboards with 2.5-Gbps transparent transponder modules and mux/demux motherboards with mux/demux modules and the OSC.

Figure 2-1 Interface Model with Splitter Protection

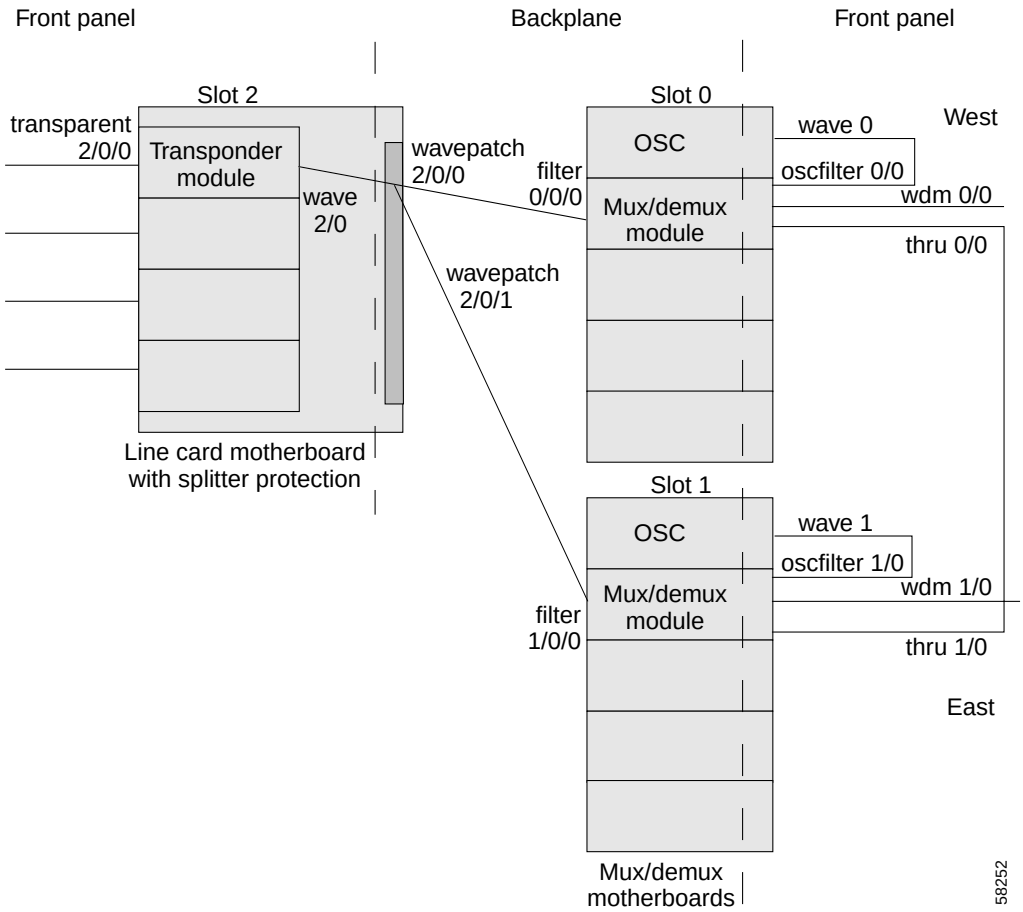
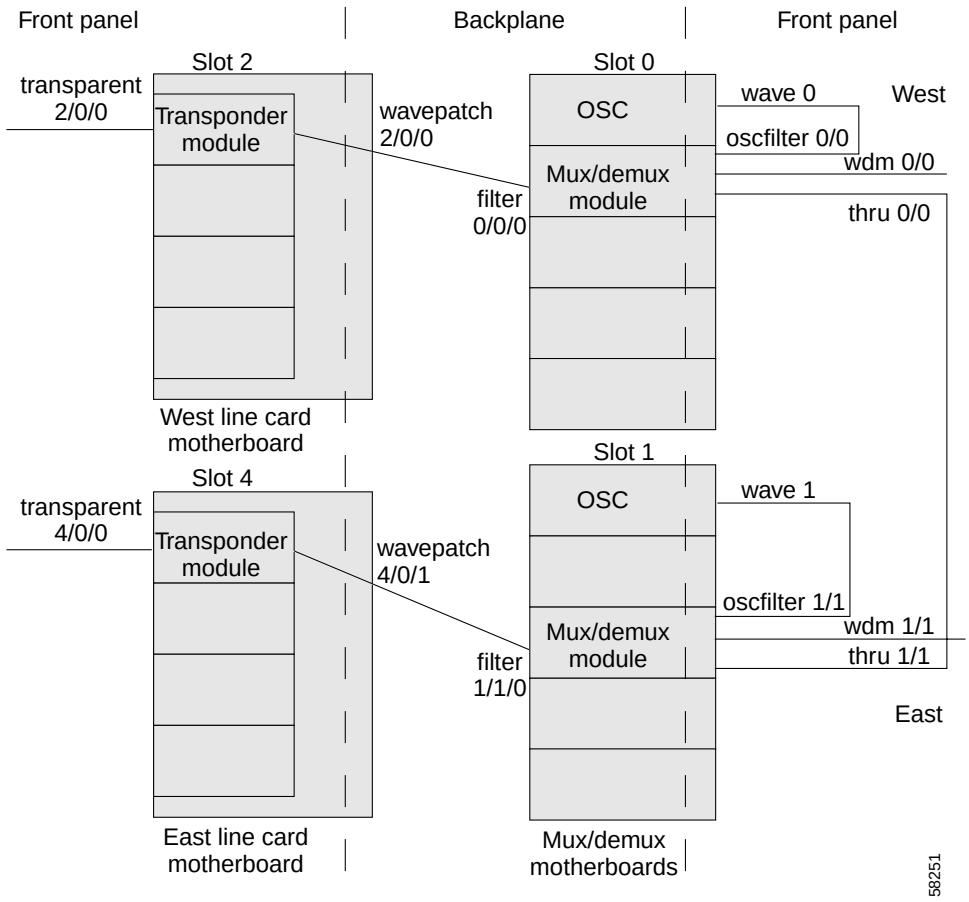


Figure 2-2 shows the interface relationship for unprotected 2.5-Gbps line card motherboards with 2.5-Gbps transparent transponder modules and mux/demux motherboards with mux/demux modules and the OSC.

Figure 2-2 Interface Model with Line Card Protection



Transparent Interfaces

The transparent interfaces are the client side interfaces on the 2.5-Gbps 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 backplane side of the 2.5-Gbps transponder module (see Figure 2-1).

The naming convention for the client side interfaces on the 2.5-Gbps transponder module is as follows:

transparent *slot*/*subcard*/*port*

Because the client side of a 2.5-Gbps transponder module has only one port, the port number is always 0. For example, the client side interface identifier for a 2.5-Gbps 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 2.5-Gbps 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 a unprotected east or west line card motherboard (see Figure 2-2).

The naming convention for wave interfaces is as follows:

wave *slot/subcard*

Wavepassthru Interfaces

The wavepassthru interface is a passive optical interface that transparently carries optical DWDM signals.

The naming convention for the wave pass thru interfaces on the ITU direct insertion module is as follows:

wavepassthru *slot/subcard/port*

Wavepatch Interfaces

The wavepatch interface is the interface on the backplane side of the line card motherboard. The wave interfaces on the backplane side of the transponder modules connect to the wavepatch interfaces.

A splitter protected line card motherboard has four pairs of wavepatch interfaces, one pair for each transponder module position. One interface of a pair connects to a filter interface on a mux/demux module in slot 0 and the other connects to a filter interface on a mux/demux module in slot 1. (See Figure 2-1.)

Unprotected line card motherboards have only one wavepatch interface per transponder module position for a total of four. A wavepatch interface on a west line card motherboard connects to the filter interface on a mux/demux module in slot 0; a wavepatch interface on an east line card motherboard connects to the filter interface on a mux/demux module in slot 1. (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*

Filter Interfaces

The filter interface is the interface on the backplane side of a mux/demux module. Each filter interface corresponds to an individual wavelength filter. The filter interface connects a wavepatch interface on a line card motherboard to a wdm interface on the same mux/demux module (see Figure 2-1).

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 15 for 16-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 represent 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 modules, to a thru interface on another add/drop mux/demux module in the same slot (see Figure 2-1).

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 a add/drop mux/demux module. The thru interface connects either to the wdm interface on an add/drop mux/demux module in the same slot, or to the thru interface on an add/drop mux/demux module in the other slot (see Figure 2-1).

The naming convention for thru interfaces is as follows:

thru *slot*/*subcard*

Filterband Interfaces

The filterband interface is an interface on the terminal mux/demux module that supports channels 1 through 16. This interface represents a pair of fibers (Rx and Tx) that transmit channels to, and receive channels from, the terminal mux/demux module that supports channels 17 through 32.

The naming convention for filterband interfaces is as follows:

filterband *slot*/*subcard*/*port*

Because each terminal mux/demux module occupies two subcard positions, the numbering for the filterband interface subcard position is either 0 or 2.

Filtergroup Interfaces

The filtergroup interface is an interface on the terminal mux/demux module that supports channels 17 through 32. This interface represents a pair of fibers (Tx and Rx) that transmit channels to, and receive channels from, the terminal mux/demux module that supports channels 1 through 16.

The naming convention for filtergroup interfaces is as follows:

filtergroup *slot*/*subcard*/*port*

Because each terminal mux/demux module occupies two subcard positions, the numbering for the filtergroup interface subcard position is either 0 or 2.

OSC Interfaces

The optional OSC provides management communications among the Cisco ONS 15540 ESP 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:

oscfilter *slot*/*subcard*

The subcard position number for an oscfilter 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 oscfilter interface. For more information on hardware rules, refer to the *Cisco ONS 15540 ESP Planning Guide.*

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 as 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. This interface is named aux 0.

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

Configuration Overview

Configure your Cisco ONS 15540 ESP systems and network using 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 ESP Hardware Installation Guide*. For detailed information on system planning and design, refer to the *Cisco ONS 15540 ESP 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 ESP 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 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. Configure the patch connections with the CLI.

For detailed information on cabling between mux/demux modules, refer to the *Cisco ONS 15540 ESP Planning Guide*. For information on configuring patch connections with the CLI, see the "Configuring Patch Connections" section on page 4-20.

Step 5 Verify the mux/demux 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 4-21 and the "About Cross Connections" section on page 4-21.

Step 6 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 protocols.

For detailed information on interface configuration, see Chapter 4, "Configuring 2.5-Gbps Transponder Module Interfaces and Patch Connections."

Step 7 Configure APS.

For detailed information on configuring APS, see Chapter 5, "Configuring Splitter Protection and Line Card Protection with APS."

Step 8 Configure processor card redundancy.

For detailed information on processor card redundancy, see the "About Processor Card Redundancy" section on page 3-15.

Step 9 Configure IP connectivity on the OSC or the in-band message channel for network management.

For detailed information on configuring IP connectivity on the OSC, see the "Configuring IP on the OSC" section on page 9-8. For detailed information on configuring connectivity on the in-band message channel, see the "Configuring SNMP" section on page 9-11.

Step 10 Configure CDP and the network topology.

For detailed information on network monitoring, see Chapter 9, "Monitoring the Network Topology".

Initial Configuration

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

About the Processor Card

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

The Cisco ONS 15540 ESP 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.

The Cisco ONS 15540 ESP 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 ESP Hardware Installation Guide*.

Starting Up the Cisco ONS 15540 ESP

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

- The system is set for the correct AC (or DC) power voltages.

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

When you start up the Cisco ONS 15540 ESP, 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 ESP 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 3-4.

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 ESP provides for 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) matches that of modem

You can configure your modem by setting the DIP switches on the modem itself or by setting them via 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: Terminal Services*.

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 ESP.

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 ESP 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 ESP 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** *password*	Sets the enable password. See the "About Passwords" section on page 3-3.
Step 5	Switch(config)# **enable password** [**level** *level*] *password*	Sets the enable password. You can specify one of 16 privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges. The default level is 15 (traditional enable privileges).
Step 6	Switch(config)# **enable secret** [**level** *level*] *password*	Specifies an enable secret password. You can specify one of 16 privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges. The default level is 15 (traditional enable privileges).
Step 7	Switch(config)# **privilege** *mode* {**level** *level* | **reset**} *command-string*	Configures or resets the privilege level to allow access to a specific command. **Note** Configure the password for a privilege level defined using the **privilege** command with the **enable secret** command.
Step 8	Switch(config-if)# **ip address** *ip-address subnet-mask*	Specifies the IP address and IP subnet mask for the management port interface.
Step 9	Switch(config-if)# **speed** {**10** | **100** | **auto**}	Specifies the transmission speed. The default is **auto** (autonegotiation).

	Command	Purpose
Step 10	Switch(config-if)# **duplex** {**auto** | **full** | **half**}	Specifies the duplex mode. The default is **auto** (autonegotiation).
Step 11	Switch(config-if)# **exit** Switch(config)#	Returns to global configuration mode.
Step 12	Switch(config)# **line vty** *line-number* 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** *password*	Specifies a password for Telnet sessions.
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 ESP 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 ESP. 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	*name*(config)# **end** *name*#	Returns to privileged EXEC mode. The prompt indicates that the host name has been set to the new name.
Step 4	*name*# **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 ESP 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.
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 ESP supports the following Cisco IOS software security features:

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

Configuring AAA

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

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 ESP 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 system, 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** *name*	Sets the host name.
Step 2	Switch(config)# **ip domain-name** *name*	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** *userid*] [**-c** {**des** | **3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc**}] [**-m** {**hmac-md5-128** | **hmac-md5-96** | **hmac-sha1-160** | **hmac-sha1-96**}] [**-o numberofpasswdprompts** *number*] [**-p** *portnumber*] [**-v** {**1** | **2**}] {*ip_address* | *hostname*} [*command*(*command*(*command*...))]	Starts the SSH client. *Command* 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 *session-id*	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
show processes	Displays active process statistics.
show processes cpu	Displays active process CPU utilization.
show processes memory	Displays active process memory utilization.

Displaying Protocols

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

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

Displaying Stacks

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

Command	Purpose
show stacks *number*	Displays system stack trace information.

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.

Displaying Environment

To display temperature and voltage information on the Cisco ONS 15540 ESP 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 ESP, use the following privileged EXEC commands:

Command	Purpose
show interface [transparent/wave/wavepatch] card/subcard/port	Displays the interface as up and in the correct state and proper counters are incrementing. There are no error counters incrementing.
show facility-alarm status	Displays alarms in the system.
show interface [osc/etherdcc] card/subcard/port	Displays management and message channel status.

Configuring Traffic Filters and Firewalls

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

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 ESP 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 ESP 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 ESP 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 arbitration:

- A newly inserted processor card always comes up as the standby processor card, except in cases where the newly inserted card is the only one present.
- If one of the processor cards cannot boot its software image, the other processor card boots as the active processor card, allowing you to correct the situation manually.
- 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

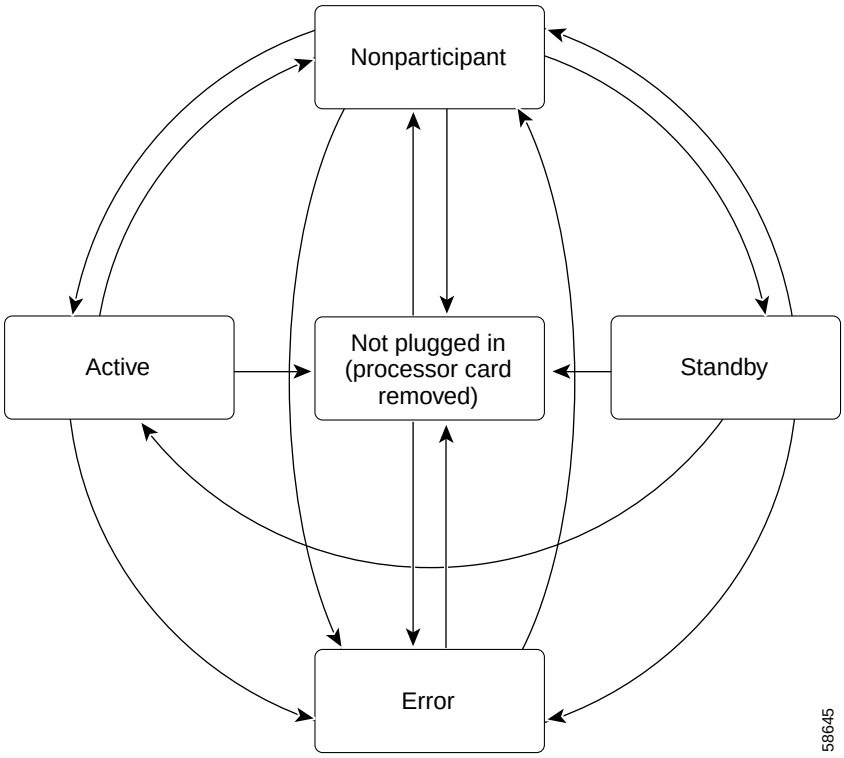
State	Description
Active	Processor card is currently providing clock signals and control for all system modules. The active processor card responds to the configured management IP address.
Standby	Processor card is partially booted in hot-standby state waiting to switch over when the active processor card fails, when it is rebooted or removed, or when a manual switchover is requested.

Table 3-1 Processor Card Hardware States (continued)

State	Description
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.
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 ESP runs in redundant mode by default. If they are not met, the system is conditionally redundant.

Note For detailed information on updating system images, refer to the *Cisco ONS 15540 ESP 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 ESP 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 ESP.

Note The initial default configuration will support 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
redundancy switch-activity [**force**]	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
switchover	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
OFTWARE
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 ESP 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 ESP 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 ESP 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 [comfirm] 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 CPU switch module CLI can be enabled from the active processor card CLI. This feature provides extra security for the Cisco ONS 15540 ESP 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
show redundancy summary	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:              15 hours, 27 minutes
sysUpTime (switchover clears): 15 hours, 27 minutes
Switchover Count:              0

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

Last Running Config sync:      never
Running Config sync status:    Disabled
Last Startup Config sync:      never
Startup Config sync status:    Disabled

This CPU is the Active CPU.
-------------------------------
Slot:                          5
Time since CPU Initialized:    15 hours, 27 minutes
Image Version:                 ONS-15540 Software (ONS15540-I-M), Release 12.1(10)EV
Image File:                    ons15540-i-mz.evt
Software Redundancy State:     ACTIVE
Hardware State:                ACTIVE
Hardware Severity:             0

Peer CPU is the Standby CPU.
-------------------------------
```

```
Slot:                          6
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:                NOT PLUGGED IN
Hardware Severity:             0
➔ Privilege Mode:              Enabled
```

About Preserving Counters on a Processor Card Switchover

The Cisco ONS 15540 ESP 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.

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, and ISC links compatibility mode traffic)	CVRD[1] error count(8b10b)
	sonet/sdh	Section code violation error count (bip1)
		Number of errored seconds (es)
		Number of severely errored seconds (ses)
		Number of severely errored framing seconds (sefs)

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 on the Processor Card Switchover

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

Command	Purpose
show redundancy capability	Displays the processor card capabilities.

Example

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

```
Switch# show redundancy capability

Standby CPU capability support (not all fields shown)

   Sby CPU                               CPU capability descriptio
 --------------------------------- --------------------------------
    48 MB                          CPU DRAM size
    16 MB                          CPU PMEM size
   512 KB                          CPU NVRAM size
    16 MB                          CPU Bootflash size

Standby linecard driver major.minor versions, (driver count=14)

 Sby CPU                      Drv/Ch/F ID  Driver description
 ---------------------------- ----------- --------------------------
 1.3                          0x1100/0/0   CPU with Switch Fabric
 2.3                          0x1101/0/0   10 Port ESCON line card
 2.1                          0x110A/0/0   8 Port GE-FC line card
 1.1                          0x1111/0/0   4 Port 2x FC line card
 3.1                          0x1105/0/0   2.5G Transparent line car
 1.9                          0x1105/1/0   2.5G Transparent line car
 3.1                          0x1109/0/0   2.5G Transparent line car
 1.9                          0x1109/1/0   2.5G Transparent line car
 1.3                          0x1103/0/0   OSC line card
 Sby CPU                      Drv/Ch/F ID  Driver description
 ---------------------------- ----------- --------------------------
 0.1                          0x1107/1/0   OSC daughter card
 2.1                          0x1102/0/0   10G trunk card
 1.0                          0x110B/0/0   2.5G trunk card
 2.1                          0x1110/0/0   PSM wdm splitter
 1.1                          0x1100/0/1   ONS15530 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.
 Sby sync client count=9)

   Sby CPU                           Cl ID  Redundancy Client descrip
 --------------------------------- ----- --------------------------
 ver  1-2                          17    CPU Redundancy
 ver  1-1                          19    Interface Sync
 ver  1-1                          36    MetOpt Password Sync
 ver  1-1                          109   MetOpt Counter Sync
 ver  1-1                          108   MetOpt Optical Cfg
 ver  1-1                          110   Metopt Crypto Sync
 ver  1-2                          18    Online Diagnostics
 ver  1-2                          6     OIR Client
 ver  1-1                          27    metopt cm db sync
```

```
Local backplane IDPROM
 Backplane IDPROM field            Local CPU
 --------------------------------- ---------------------------------
 idversion                         1
 magic                             153
 card_type                         4358
 order_part_num_str                PROTO-HAMPTON-CHASSIS
 description_str                   Prototype Hampton Backplane
 board_part_num_str                73-6573-03
 board_revision_str                02
 serial_number_str                 TBC055089
 date_of_manufacture_str           10/21/2001
 deviation_numbers_str             N/A
 manufacturing_use                 0
 rma_number_str
 rma_failure_code_str
 oem_str                           Cisco
 clei_str                          TBD
 snmp_oid_substr                   TBD
 schematic_num_str                 92-4568-03
 hardware_major_version            3
 Backplane IDPROM field            Local CPU
 --------------------------------- ---------------------------------
 hardware_minor_version            1
 engineering_use_str               LAB Prototype
 crc16                             52960
 user_track_string                 hello PhyAlias  test AssetTag123
 diagst                            ^A
 board_specific_revision           1
 board_specific_magic_number       153
 board_specific_length             56
 mac_address_block_size            16
 mac_address_base_str              00016447a240
 cpu_number                        0
 optical_backplane_type            255


List of Configurable features and their current status:

Redundancy Client        Feature             Enabled/Disabled
-----------------        -------             -----------------
MetOpt Counter Sync      Counter Sync        Enabled

Switch#
```

About the Software Configuration Register

The Cisco ONS 15540 ESP 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
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.

Table 3-8 Configuration Register Boot Field Values (continued)

Boot Field Value	Description
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 ESP 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, refer to the *Cisco ONS 15540 ESP 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** *value*	Sets the contents of the configuration register. The *value* 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 ESP 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 cards.

If a single fan fails, a minor alarm is reported to the processor card. However, the chassis will never reach a 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 reset or power off the transponder modules. The transponder modules power off if the hardware version of the line card motherboard is 5.1 or later; otherwise, the 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
environment-monitor shutdown fan	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
show environment	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     Critcal   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 ESP 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 ESP 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 (º C)	Air Outlet Sensor Threshold Temperature in degree Celsius (º 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 ESP system automatically shuts down the 2.5-Gbps transponder cards if the operating temperature exceeds the critical threshold. 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 *slot/subslot/module*	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} *slot/subslot/module <threshold value>*	Sets new[1] threshold temperatures for the specified temperature sensor 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 temperature sensor modules, use the following global configuration command:

Command	Purpose
no environment-monitor temperature-threshold	Resets all thresholds to the default temperatures for all temperature sensor 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                 Thresholds
                              (degree C)    Minor      Major     Critcal   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
                                          Minor   Major   Critical  Mode
--------------------  ------  -------  ----------------------  --------
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
```

CHAPTER 4

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 ESP. This chapter includes the following sections:

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

Step 1 Configure the patch connections between the mux/demux modules (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** *slot*/*subcard*/**0** Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# **encapsulation** {**fastethernet** | **fddi** | **gigabitethernet** | **escon**} or	Specifies Fast Ethernet, FDDI, Gigabit Ethernet, or ESCON. OFC[1] is disabled.
	Switch(config-if)# **encapsulation sysplex clo** or	Specifies Sysplex CLO[2]. OFC is disabled. Forward laser control is enabled on both the transparent and wave interfaces. OFC is disabled.
	Switch(config-if)# **encapsulation sysplex etr** or	Specifies Sysplex ETR[3]. OFC is disabled.
	Switch(config-if)# **encapsulation sysplex isc** {**compatibility** | **peer [1g** | **2g]**} or	Specifies ISC[4] compatibility mode (1 Gbps) or peer mode (1 Gbps or 2 Gbps). OFC is enabled for compatibility mode and disabled for peer mode.
	Switch(config-if)# **encapsulation ficon** {**1g** | **2g**} or	Specifies FICON and 1 Gbps or 2 Gbps as the transmission rate. OFC is disabled.
	Switch(config-if)# **encapsulation sonet** {**oc3** | **oc12** | **oc48**} or	Specifies SONET as the signal protocol and OC-3, OC-12, or OC-48 as the transmission rate. OFC is disabled.
	Switch(config-if)# **encapsulation sdh** {**stm-1** | **stm-4** | **stm-16**} or	Specifies SDH as the signal protocol and STM-1, STM-4, or STM-16 as the transmission rate. OFC is disabled.
	Switch(config-if)# **encapsulation fibrechannel** {**1g** | **2g**} [**ofc** {**enable** | **disable**}] or	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.
	Switch(config-if)# **clock rate** *value*	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 4-12.
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 ESP 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.

Sysplex CLO and Sysplex ETR are supported outside the nominal range of the clock rates for the Cisco ONS 15540 ESP 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	1,244,160
SONET OC-48/SDH 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 ESP 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 2.5-Gbps 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.

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 5, "Configuring Splitter Protection and Line Card Protection with 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 *slot*/*subcard*/**0**	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 ESP 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 and peer 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 GE, FC, and FICON traffic, the Cisco ONS 15540 ESP 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 ESP monitors the SONET section overhead only, not the SONET line overhead. Specifically, the Cisco ONS 15540 ESP 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:

- 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.

Example

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.

Example

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 2.5-Gbps 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** *name* 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** *seconds*	Configures the SNMP notification timer. The default value is 5 seconds. (Optional)
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.

	Command	Purpose
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 4-2 lists the threshold error rates in errors per second for each of the protocol encapsulations.

Table 4-2 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	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)# encap 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)# encap 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 [*name*]	Displays the threshold group configuration.
show interfaces {**transparent** *slot*/*subcard*/**0** | **wave** *slot*[/*subcard*]}	Displays the transparent or wave interface configuration.

Example

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

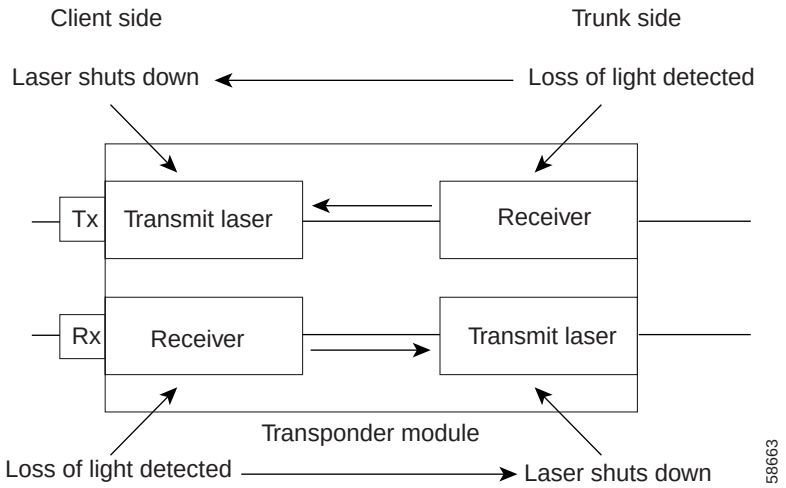
To avoid operator injury or transmission of unreliable data, or to provide quick path switchover, the Cisco ONS 15540 ESP supports mechanisms to automatically shut down 2.5-Gbps transponder module lasers. The three types of laser shutdown mechanisms are:

- 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:

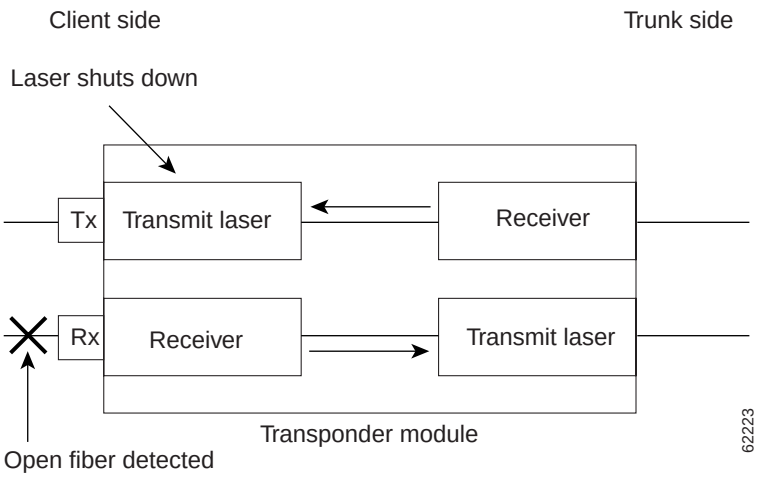
- Sysplex ETR
- Sysplex CLO
- Sysplex ISC peer mode
- All Y-cable automatic protection switching configurations

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 ESP 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 2.5-Gbps 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 ESP interoperates with OFC-standard-compliant client equipment.

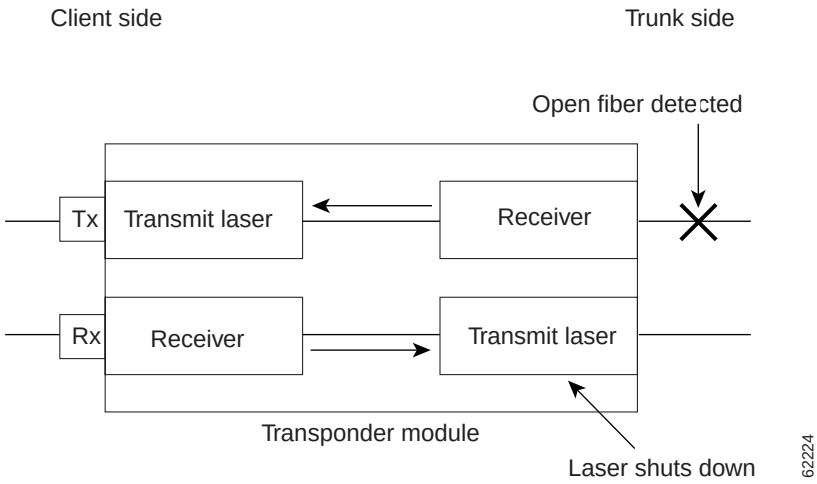
Caution Do not configure OFC with either forward laser control or laser safety control. Combining these features interferes with the OFC protocol.

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 ESP allows you to enable laser safety control on the trunk side interfaces of the 2.5-Gbps transponder modules. Much like OFC, the laser safety control protocol shuts down the 2.5-Gbps 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 2.5-Gbps transponder module interfaces.

Note To function correctly, configure forward laser control on both the transparent and wave interfaces on a 2.5-Gbps transponder module. For y-cable protection, configure forward laser control on both the transparent and wave interfaces on both 2.5-Gbps transponder modules.

Configuring Forward Laser Control

To configure forward laser control on a 2.5-Gbps transponder module transparent and wave interfaces, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **interface transparent** *slot*/*subcard*/*port* 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** *slot*[/*subcard*] 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 2.5-Gbps 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** *slot*/*subcard*/*port* | **wave** *slot*/*subcard*}	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** {*slot* | *slot/subcard*} Switch(config-if)#	Selects the wave interface to configure and enters interface configuration mode.
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 {*slot* | *slot/subcard*}	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 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 transponder module, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **interface wavepatch** *slot/subcard/port* 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 wavepatch interfaces 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 *slot/subcard/port*	Displays interface information.

Example

The following example shows how to display the optical power threshold 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 ESP 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, no CLI configuration is necessary for the signal to pass from the client to the trunk fiber.

Table 4-3 describes the types of patch connections on the Cisco ONS 15540 ESP.

Table 4-3 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

Table 4-3 Patch Connection Types (continued)

Patch Connection	Description
Filterband interface to filtergroup interface or filtergroup interface to filterband interface	Connection between the terminal mux/demux module supporting channels 1 through 16 and the terminal mux/demux module supporting channels 17 through 32 in the same chassis slot or 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 the mux/demux motherboard and the OSC oscfilter interface on the mux/demux module in the same chassis slot

For more information on patch connection rules, refer to the *Cisco ONS 15540 ESP Planning and Design 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 *slot/subcard1* **wdm** *slot/subcard2* or **patch wdm** *slot/subcard1* **thru** *slot/subcard2*	Configures the patch connection between two add/drop mux/demux modules in the same chassis slot.
patch thru *slot1/subcard1* **thru** *slot2/subcard2*	Configures the patch connection between two add/drop mux/demux modules in different chassis slots.
patch filterband *slot1/subcard1/port1* **filtergroup** *slot2/subcard2/port2* or **patch filtergroup** *slot1/subcard1/port1* **filterband** *slot2/subcard2/port2*	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.
patch wave *slot* **oscfilter** *slot/subcard* or **patch oscfilter** *slot/subcard* **wave** *slot*	Configures the patch connection between the OSC wave interface on the mux/demux motherboard and the OSC oscfilter interface on the mux/demux module in the same chassis slot.

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 9-3.

Example

The following example shows how configure the patch connections between OSC interfaces and between mux/demux modules:

```
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
```

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 2.5-Gbps 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:

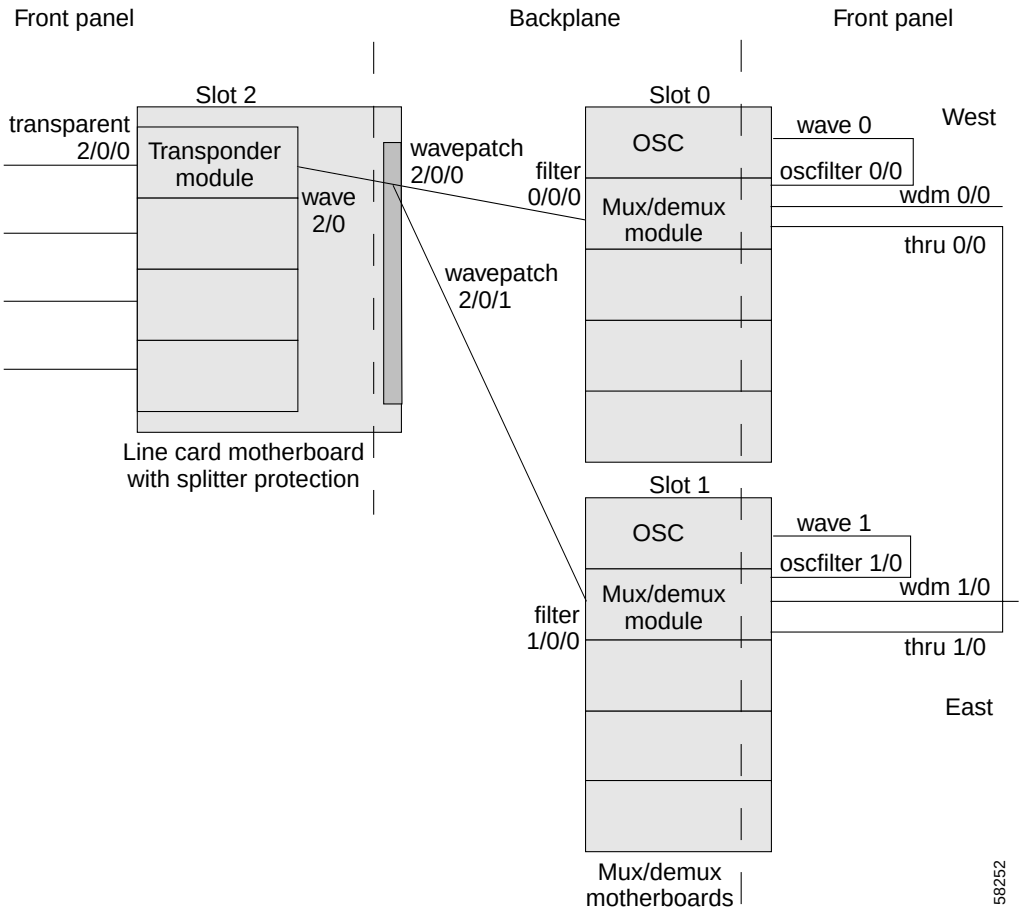
```
Switch# show patch

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 interface optical cross connections through the Cisco ONS 15540 ESP. Figure 4-4 shows an example of cross connections. Knowing the path of a signal through the shelf helps with system management and troubleshooting.

Figure 4-4 Optical Cross Connection Example



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** {**transparent** *slot/subcard/port* | **wave** *slot/subcard*}]]	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
Trans2/2/0    Wave2/2        2/2/0*  0/0/2   0/0    3
                             2/2/1   1/0/2   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    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 ESP supports 15 minute based performance history counters. You can use the performance history counters to track the performance of the Cisco ONS 15540 ESP interfaces.

There are three types of performance history counters: current, 15-minute history, and 24-hour. Cisco ONS 15540 ESP 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 ESP 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 ESP 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 [*interface*]	Displays the current counter for the specified interface[1].
show performance history [*interface*] [*interval number*]	Displays the 15-minute history counter for the specified interface and interval number[1].
show performance 24-hour [*interface*]	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 [*interface*]	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
```

CHAPTER 5

Configuring Splitter Protection and Line Card Protection with 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

APS provides protection against signal transmission failure. The Cisco ONS 15540 ESP supports the following APS features:

- 1+1 path protection
- Splitter protection
- Line card protection
  - Client based
  - Y-cable based
- Bidirectional and unidirectional path switching

The 1+1 path protection architecture transmits the client signal on both the working and protection paths.

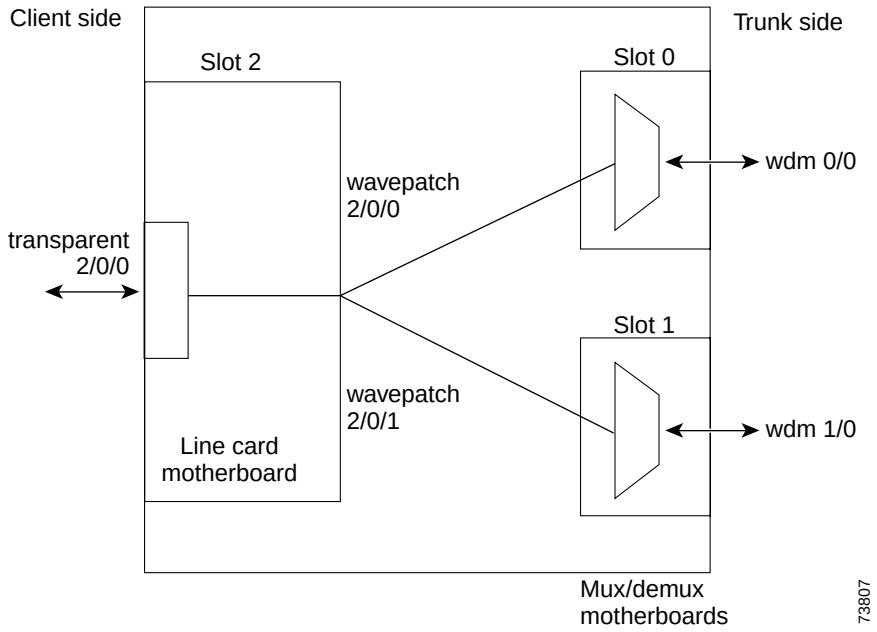
Note For an animated description of the APS implementation on the Cisco ONS 15540 ESP, go to the following URL:

http://www.cisco.com/mm/dyngraph/APS15540.html

About Splitter Protection

Splitter protection on the Cisco ONS 15540 ESP 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 5-1).

Figure 5-1 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 motherboard 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 ESP 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 5-6 and the "Configuring Y-Cable Based Line Card Protection" section on page 5-8. 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.
- 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 ESP 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 ESP 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 4-19.

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 4-19.

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**]	Configures APS splitter protection mode on the entire chassis. The default state is disabled.
	or	or
	Switch(config-red)# **associate interface wavepatch** *slot*/*****/*working-interface* **wavepatch** *slot*/*****/*protection-interface* [**enable** | **disable**]	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/*/0 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** *name* | **interface wavepatch** *slot/subcard/port*}	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 ESP 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 ESP supports three types of line card protection:

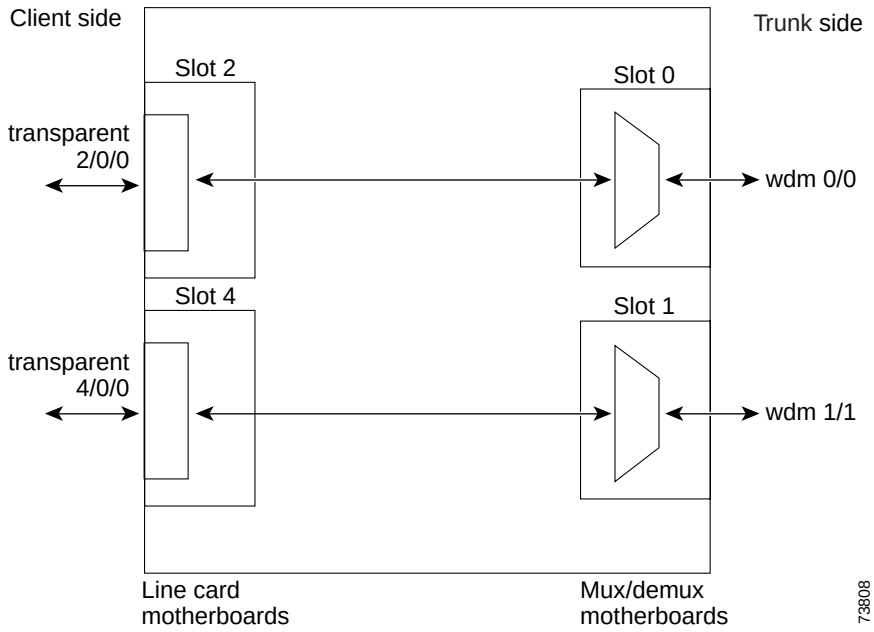
- Client based protection
- Y-cable protection

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 ESP.

Figure 5-2 Line Card Protection Scheme with 2.5-Gbps Transponder Module



The Cisco ONS 15540 ESP 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 ESP.

With y-cable protection, the signal from only one of the transparent interfaces is transmitted to the client. The Cisco ONS 15540 ESP 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 ESP 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 ESP 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.

  For more information about dual shelf nodes, see Chapter 6, “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 ESP 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 5-7.)

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 ESP 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* | **tengigethernetphy** *slot/subcard*}	Configures the working path interface.
Step 5	Switch(config-red-aps)# **aps protection** {**transparent** *slot/subcard/port* | **tengigethernetphy** *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
show aps	Displays the APS configuration summary.
show aps {**detail** | **group** *name* | **interface** {**transparent** *slot/subcard*/**0** | **tengigethernetphy** *slot/subcard*}}	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
```

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** *slot/subcard/port* 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 5-2 on page 5-6 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)#
```

Configuring APS Group Attributes

This section describes APS group attributes and how to configure them.

Configuring Revertive Switching

The Cisco ONS 15540 ESP supports revertive switching for all types of 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.

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** | **wavepatch** *slot*/*subcard*/*port* | **tengigethernetphy** *slot*/*subcard*}]	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): Transparent7/0/0 (STANDBY - UP), Wave7/0 (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 ESP 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 ESP 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 ESP implements path switching using an APS channel protocol over the OSC (optical supervisory channel) on the protection path, or the IP management connection.

Note Bidirectional path switching operates only on Cisco ONS 15540 ESP networks that have the OSC or the IP management connect. You must also configure the patch connection between the OSC and the mux/demux motherboard if you use the OSC as the APS message channel.

Figure 5-3 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 5-3 Active and Standby Path Configuration Example

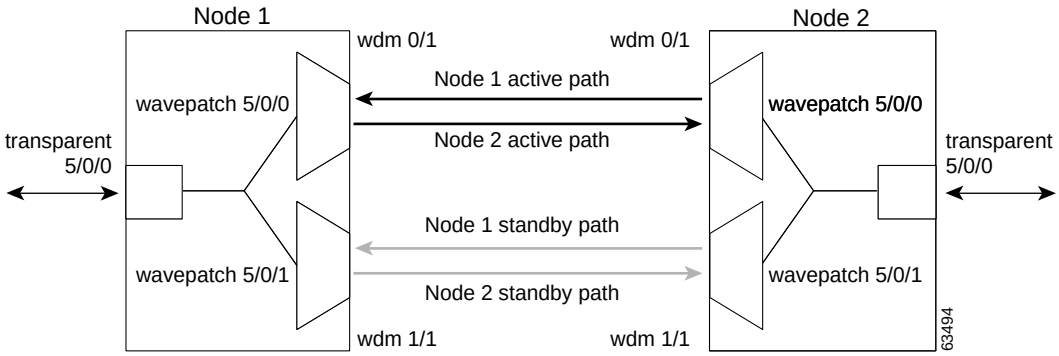


Figure 5-4 shows the behavior of unidirectional path switching when a loss of signal occurs. For the two node example network, unidirectional path switching operates as follows:

- 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 5-4 Unidirectional Path Switching Example

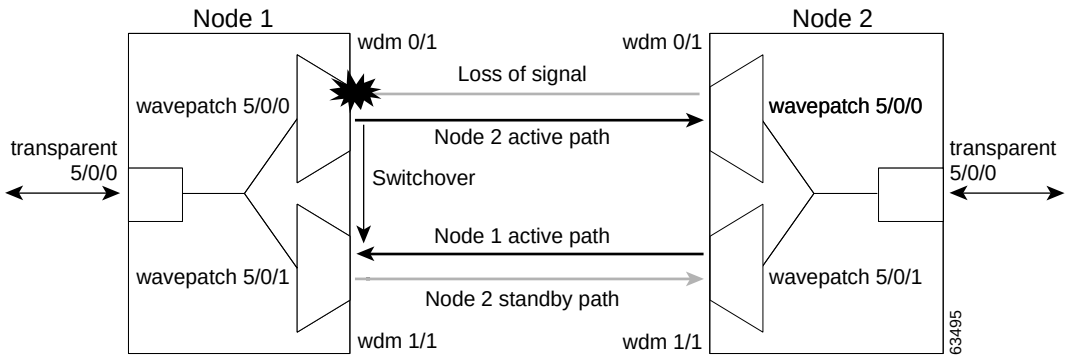
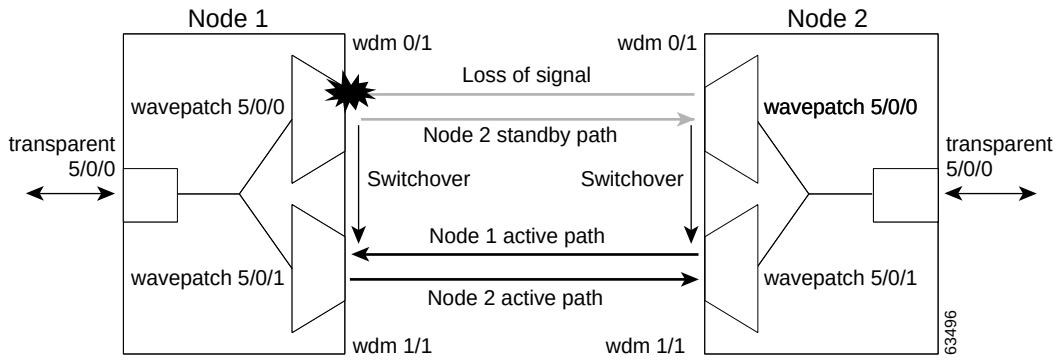


Figure 5-5 shows the behavior of bidirectional path switching when a loss of signal occurs. For the two node example network, bidirectional path switching operates as follows:

- 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 5-5 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*}	Configures the working path interface.
Step 6	Switch(config-red-aps)# **aps protection** {**transparent** *slot*/*subcard*/**0** | **wavepatch** *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.

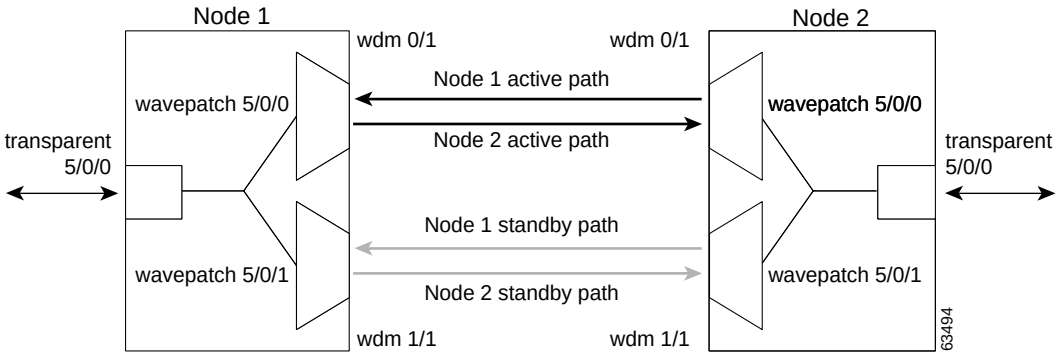
Note Both nodes in the network that add and drop the channel must have the same APS configuration. Specifically, both must have the same path switching behavior, and working and protection paths.

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 5-6 shows the active and standby paths between node 1 and node 2 with splitter protection.

Figure 5-6 Bidirectional Path Switching Example with Splitter Protection



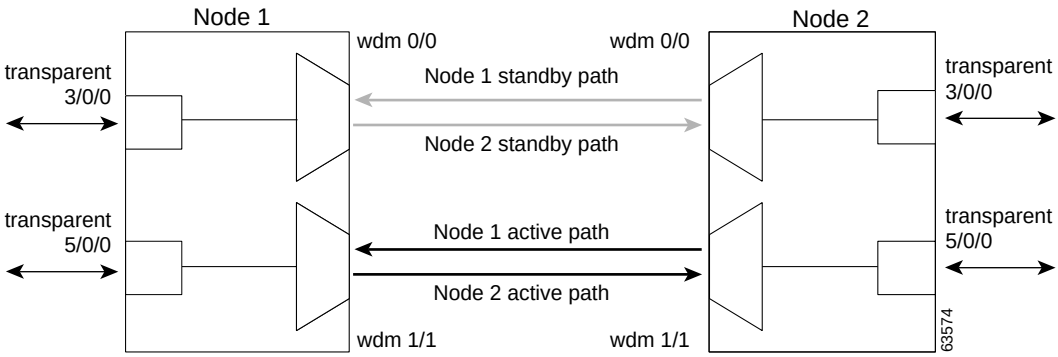
The following example shows how to configure one channel in the example network for bidirectional path switching using the default working and protection path interfaces:

```
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 5-7 shows the active and standby paths between node 1 and node 2 with y-cable protection.

Figure 5-7 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** *name*	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** *slot*/*subcard*/**0** 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** *name* 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.
Step 12	Switch(config-red)# **exit** Switch(config)#	Exits redundancy configuration mode.

	Command	Purpose
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*}]	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 ESP 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** *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 switchover-enable min-interval** *seconds*	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*}]	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 ESP 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** *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 wait-to-restore** *seconds*	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 yc
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** *name* | **interface** {**transparent** *slot*/*subcard*/**0** | **wavepatch** *slot*/*subcard*/*port* | **tengigethernetphy** *slot*/*subcard*}]	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 ESP 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** *slot*/*subcard*/**0** | **wavepatch** *slot*/*subcard*/*port*|**tengigethernetphy** *slot*/*subcard*]	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 ESP 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** *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 message holddown** *milliseconds* [**count** *number*]	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** *seconds*	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** *name* | **interface** {**transparent** *slot/subcard/***0** | **wavepatch** *slot/subcard/port* | **tengigethernetphy** *slot/subcard*]	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 ESP 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
aps lockout *group-name*	Locks out all switchovers to the protection path.
aps switch *group-name* {**force** | **manual**} {**protection-to-working** | **working-to-protection**}	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
show aps [**detail** | **group** *name* | **interface** {**transparent** *slot/subcard/***0** | **wavepatch** *slot/subcard/port* | **tengigethernetphy** *slot/subcard*}}]	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
aps clear *group-name*	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
show aps [**detail** | **group** *name* | **interface** {**transparent** *slot*/*subcard*/**0** | **wavepatch** *slot*/*subcard*/*port* | **tengigethernetphy** *slot*/*subcard*}]	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
```

CHAPTER 6

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

On a single Cisco ONS 15540 shelf, only 16 channels can be supported with line card protection. By cascading two Cisco ONS 15540 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 4-19.

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 3-4.

Step 4 Configure IP addresses on the OSC wave interfaces.

For information on configuring IP address on the OSC wave interface, see the "Configuring IP on the OSC" section on page 9-8.

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

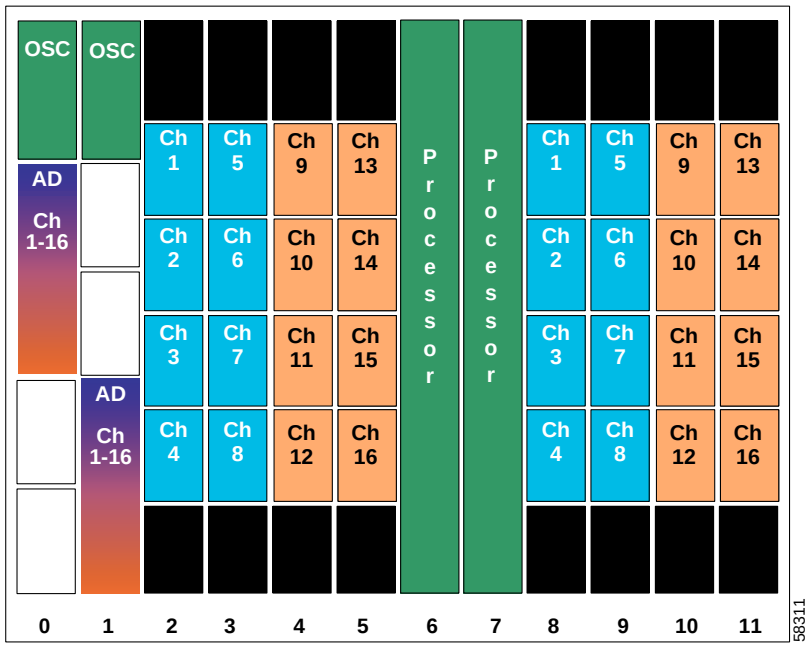
You can use either terminal or add/drop mux/demux modules in a dual shelf node. For configurations with 32 channels with line card protection, we recommend using the 16-channel terminal mux/demux module. For configurations with fewer than 32 channels in line card protection, use 8-channel add/drop mux/demux modules as often as possible.

Terminal Mux/Demux Modules for 32-Channels

Shelf 1 is configured for channels 1–16 with OSC, while shelf 2 is configured for channels 17–32 without OSC. The mux/demux modules are patched between the two shelves as if they were in the same shelf.

Figure 6-1 shows how the modules are installed for shelf 1 in the line card protected 32-channel configuration.

Figure 6-1 Shelf 1 Configuration for 32 Channels with Terminal Mux/Demux Modules and Line Card Protection



The configuration for shelf 2 is shown in Figure 6-2. As in shelf 1, the west line card motherboards are used in slots 2–5, and the east line card motherboards are used in slots 8–11.

Figure 6-2 Shelf 2 Configuration for 32 Channels with Terminal Mux/Demux Modules and Line Card Protection

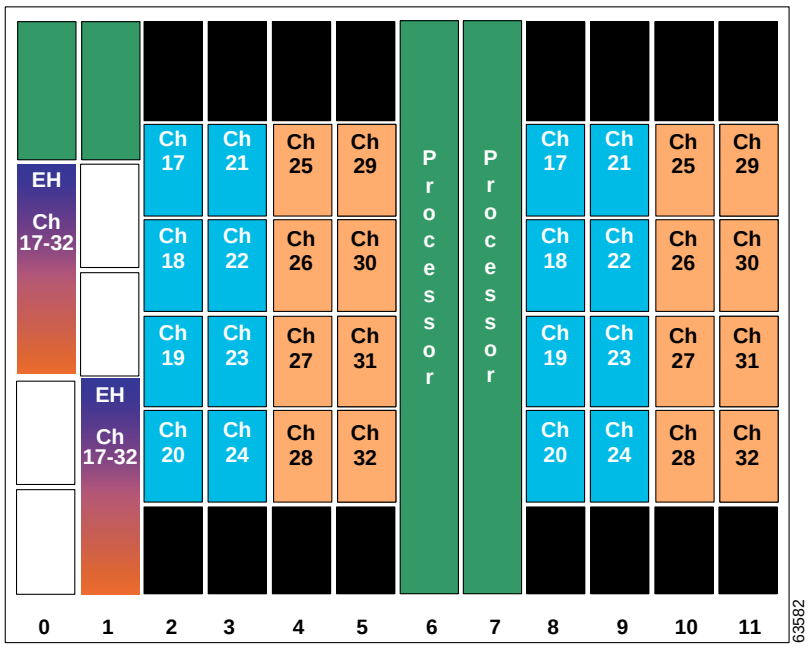
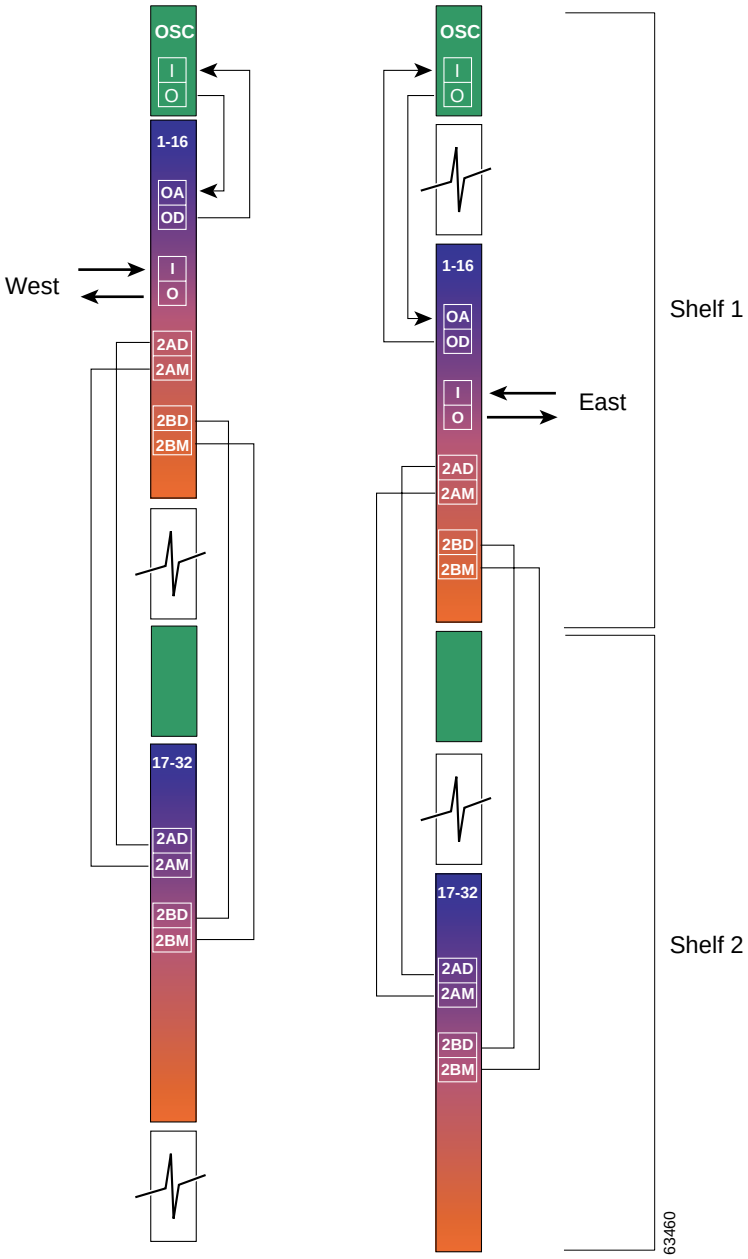


Figure 6-3 shows how the terminal mux/demux modules are cabled between the two shelves to support all 32 channels on both the east and west sides.

Figure 6-3 Terminal Mux/Demux Module Cabling with Two Shelves with 32 Channels and Line Card Protection

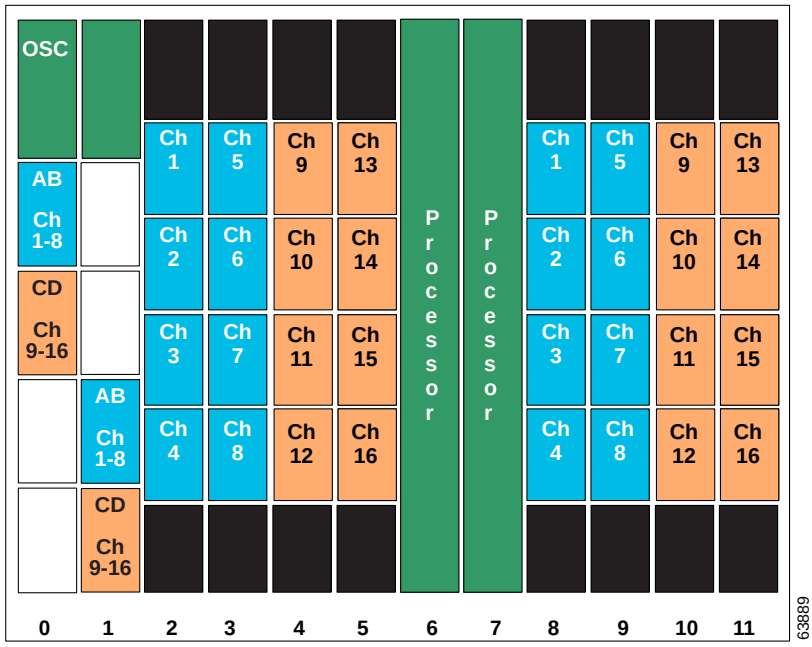


Add/Drop Mux/Demux Modules for 24-Channels

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 6-4 shows how the modules are installed for shelf 1 in the line card protected 24-channel configuration.

Figure 6-4 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 6-5. As in shelf 1, the west line card motherboards are used in slots 2–5, and the east line card motherboards are used in slots 8–11.

Figure 6-5 Shelf 2 Configuration for 24 Channels with Add/Drop Mux/Demux Modules and Line Card Protection

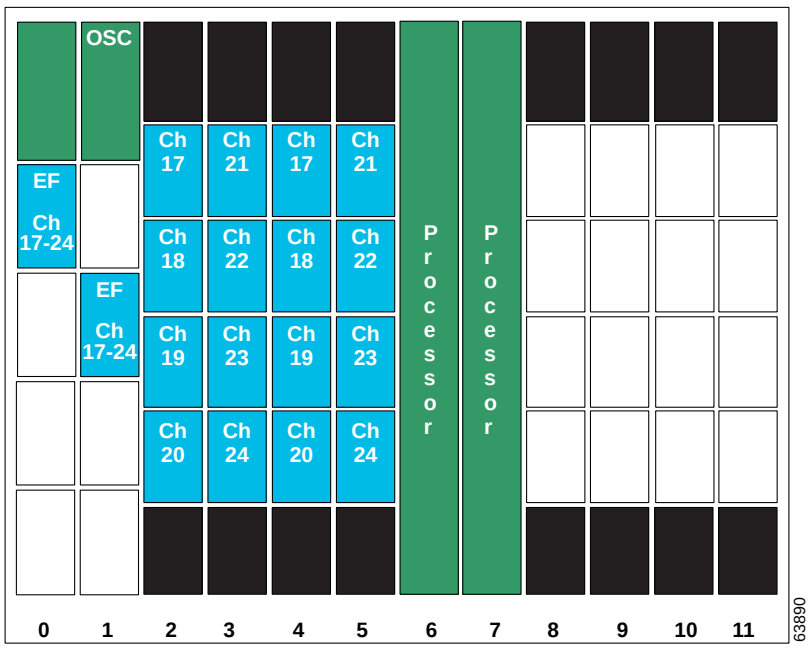
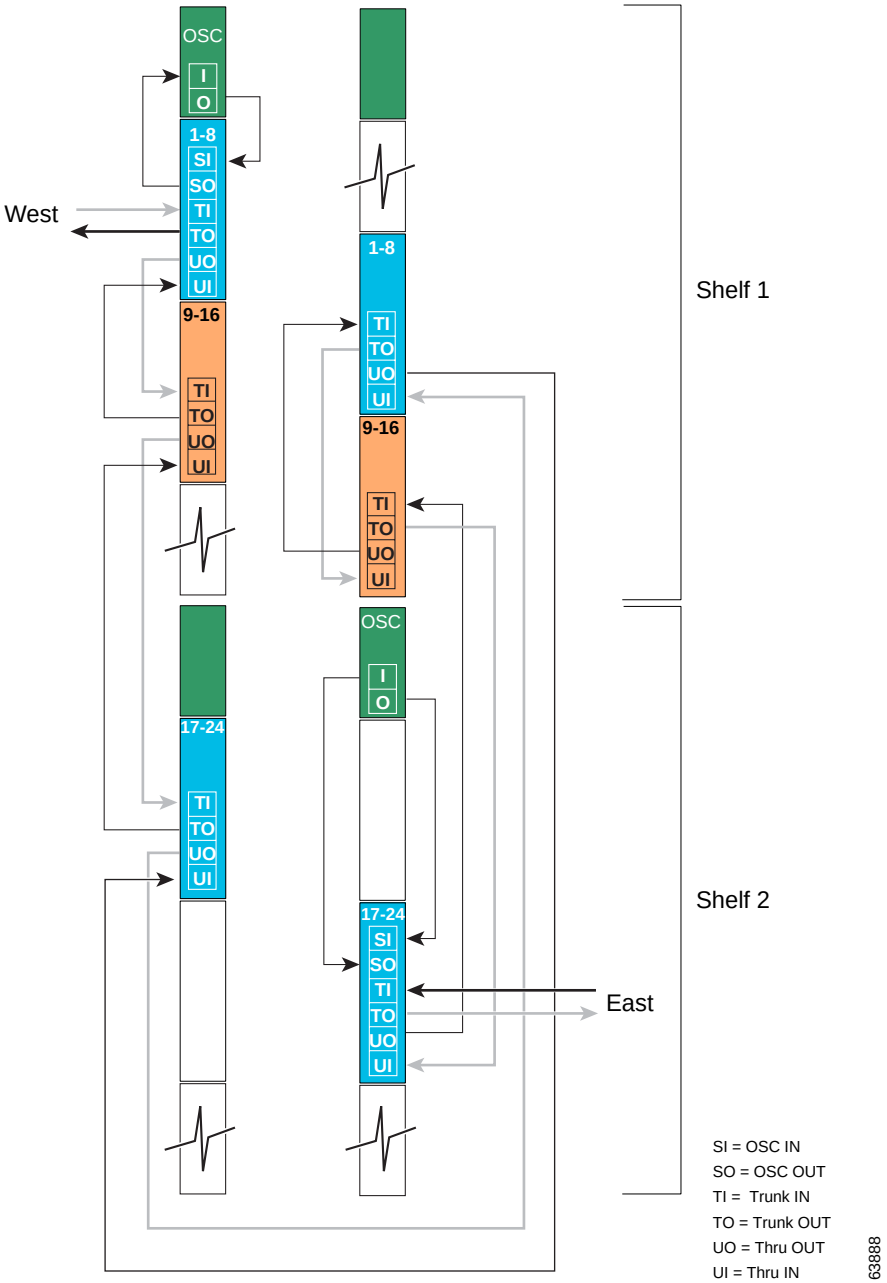


Figure 6-6 shows how the terminal mux/demux modules are cabled between the two shelves to support 24 channels on both the east and west sides.

Figure 6-6 Add/Drop Mux/Demux Module Cabling with Two Shelves with 24 Channels and Line Card Protection



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** {**wave** *slot* | **oscfilter** *slot/subcard* | **thru** *slot/subcard* | **wdm** *slot/subcard* | **filterband** *slot/subcard/port* | **filtergroup** *slot/subcard/port*}	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.

Note Configure the patch connections between the mux/demux modules on the same shelf as described in the "Configuring Patch Connections" section on page 4-20.

Examples

The following example shows how to configure the patch connections between the terminal mux/demux modules on the two shelves in the node:

```
Shelf1(config)# interface filterband 0/0/0
Shelf1(config-if)# topology neighbor name shelf2 port name filtergroup 0/0/0
Shelf1(config-if)# topology neighbor agent ip-address 10.1.2.3
Shelf1(config-if)# exit
Shelf1(config)# interface filterband 0/0/1
Shelf1(config-if)# topology neighbor name shelf2 port name filtergroup 0/0/1
Shelf1(config-if)# topology neighbor agent ip-address 10.1.2.3
Shelf1(config-if)# exit
Shelf1(config)# interface filterband 1/2/0
Shelf1(config-if)# topology neighbor name shelf2 port name filtergroup 1/2/0
Shelf1(config-if)# topology neighbor agent ip-address 10.1.2.3
Shelf1(config-if)# exit
Shelf1(config)# interface filterband 1/2/1
Shelf1(config-if)# topology neighbor name shelf2 port name filtergroup 1/2/1
Shelf1(config-if)# topology neighbor agent ip-address 10.1.2.3

Shelf2(config)# interface filtergroup 0/0/0
Shelf2(config-if)# topology neighbor name shelf1 port name filterband 0/0/0
Shelf2(config-if)# topology neighbor agent ip-address 10.2.2.4
Shelf2(config-if)# exit
Shelf2(config)# interface filtergroup 0/0/1
Shelf2(config-if)# topology neighbor name shelf1 port name filterband 0/0/1
Shelf2(config-if)# topology neighbor agent ip-address 10.2.2.4
Shelf2(config-if)# exit
Shelf2(config)# interface filtergroup 1/2/0
Shelf2(config-if)# topology neighbor name shelf1 port name filterband 1/2/0
```

```
Shelf2(config-if)# topology neighbor agent ip-address 10.2.2.4
Shelf2(config-if)# exit
Shelf2(config)# interface filtergroup 1/2/1
Shelf2(config-if)# topology neighbor name shelf1 port name filterband 1/2/1
Shelf2(config-if)# topology neighbor agent ip-address 10.2.2.4
```

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 6-4 on page 6-5, or no OSC connections at all, such as the configuration shown in Figure 6-2 on page 6-3. 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** *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 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** *slot/subcard/port*	Configures the working path interface.
Step 5	Switch(config-red-aps)# **aps protection wavepatch** *slot/subcard/port*	Configures the protection path interface.

	Command	Purpose
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** *group-name* **ip-address** *address*	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 "About Line Card Protection" section on page 5-6.

Examples

For these examples, assume the following:

- Channels 17-20 terminate on the second shelf of the dual shelf node.
- The second shelf of the dual shelf node has no OSC support (see Figure 6-3 on page 6-4).
- 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

In a point-to-point topology, two Cisco ONS 15540 ESP 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 7-1 shows an example of this topology using two DWDM fiber links, one working and one protection.

Figure 7-1 Protected Point-to-Point Topology Example

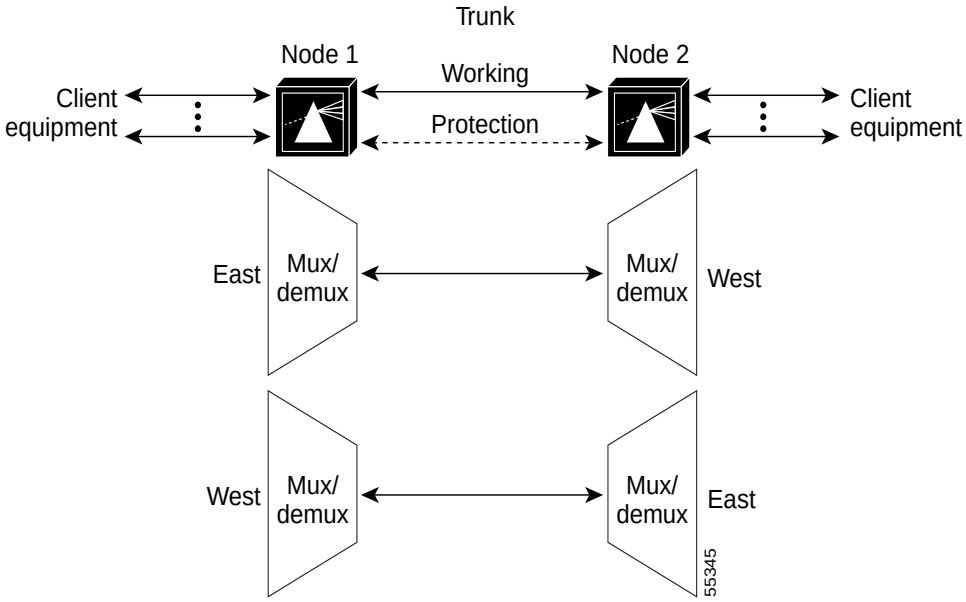
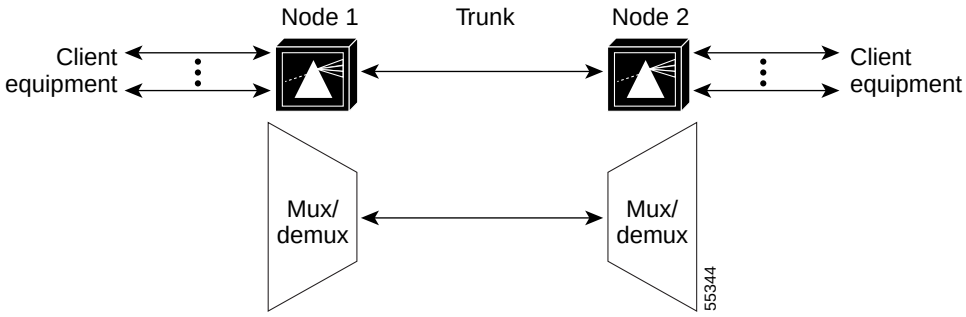


Figure 7-2 shows an example of an unprotected point-to-point topology using one unprotected DWDM fiber link.

Figure 7-2 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 ESP Planning and Design Guide*.

Configuring a Point-to-Point Topology with Splitter Protection

Figure 7-3 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 7-3 Shelf Configuration for Splitter Protected 32-Channel Point-to-Point Topology

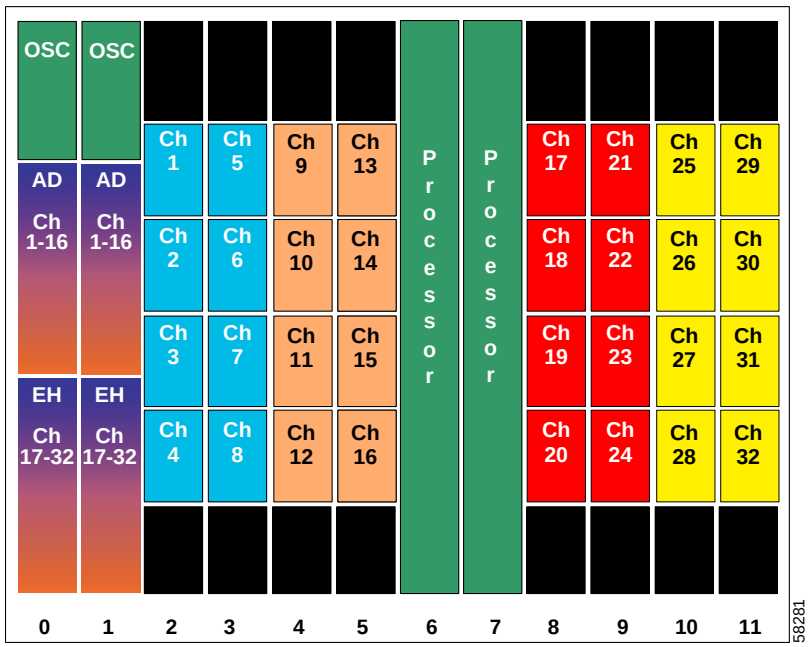
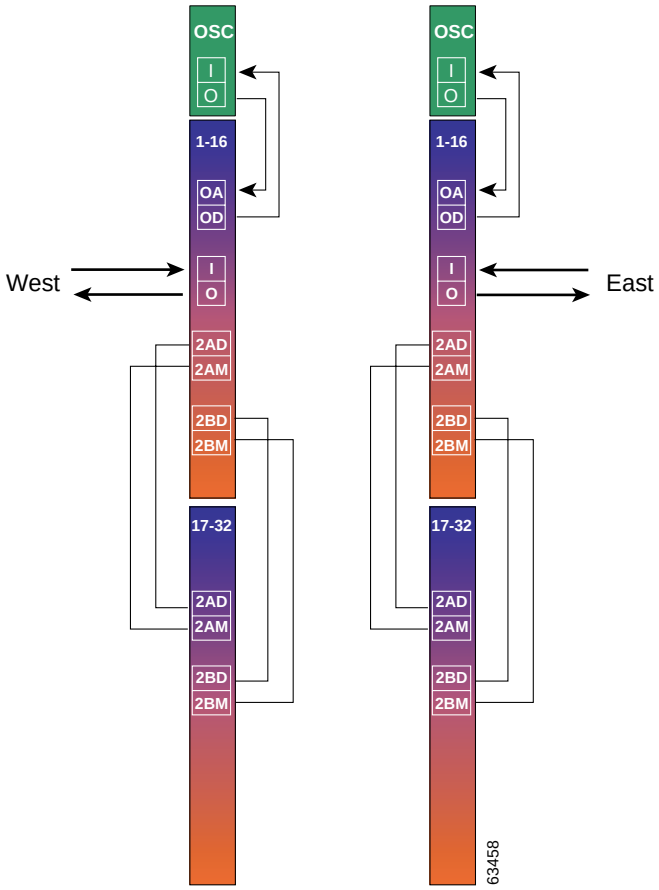


Figure 7-4 shows how the terminal mux/demux modules are cabled for the 32-channel splitter protected point-to-point configuration.

Figure 7-4 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 filterband 0/0/0 filtergroup 0/2/0
Node1(config)# patch filterband 0/0/1 filtergroup 0/2/1
Node1(config)# patch filterband 1/0/0 filtergroup 1/2/0
Node1(config)# patch filterband 1/0/1 filtergroup 1/2/1
```

Transparent Interfaces

```
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>
```

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 7-5 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 7, "Configuring Point-to-Point Topologies."

Figure 7-5 Shelf Configuration for Line Card Protected 32-Channel Point-to-Point Topology

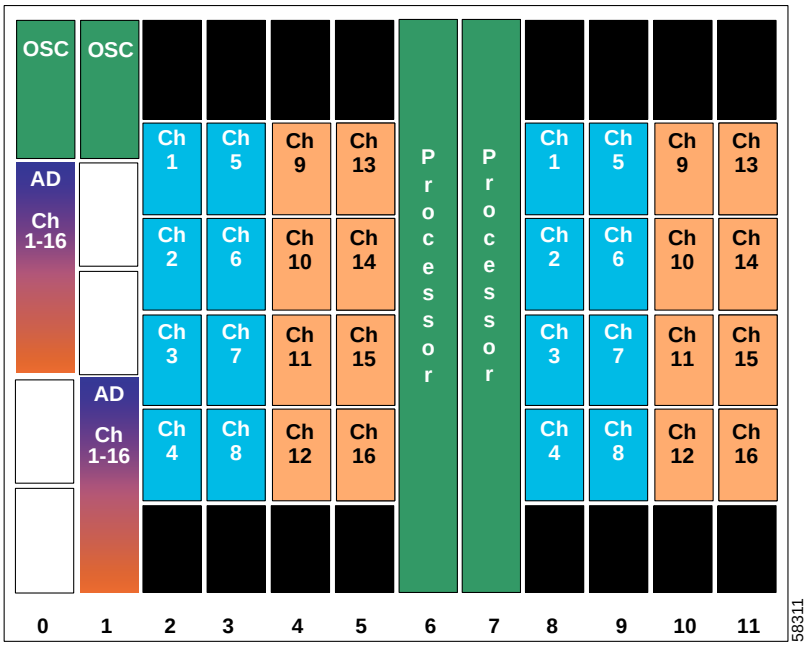
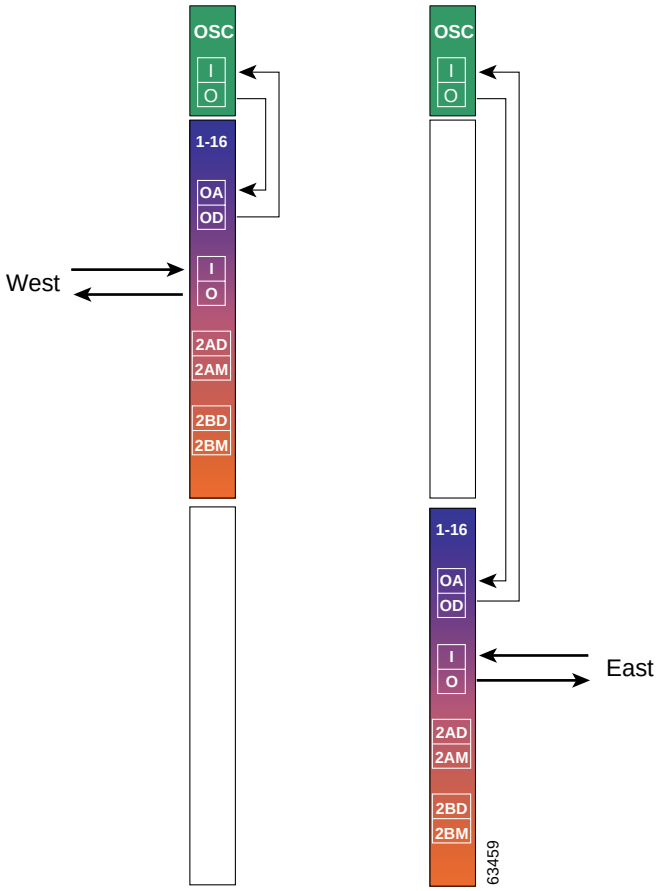


Figure 7-6 shows how the terminal mux/demux modules are cabled for the 16-channel line card protected point-to-point configuration.

Figure 7-6 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 1/2
```

Transparent Interfaces

```
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>
```

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 7-7 shows how the modules are installed in the shelf for a 32-channel point-to-point topology without protection.

Figure 7-7 Shelf Configuration for Unprotected 32-Channel Point-to-Point Topology

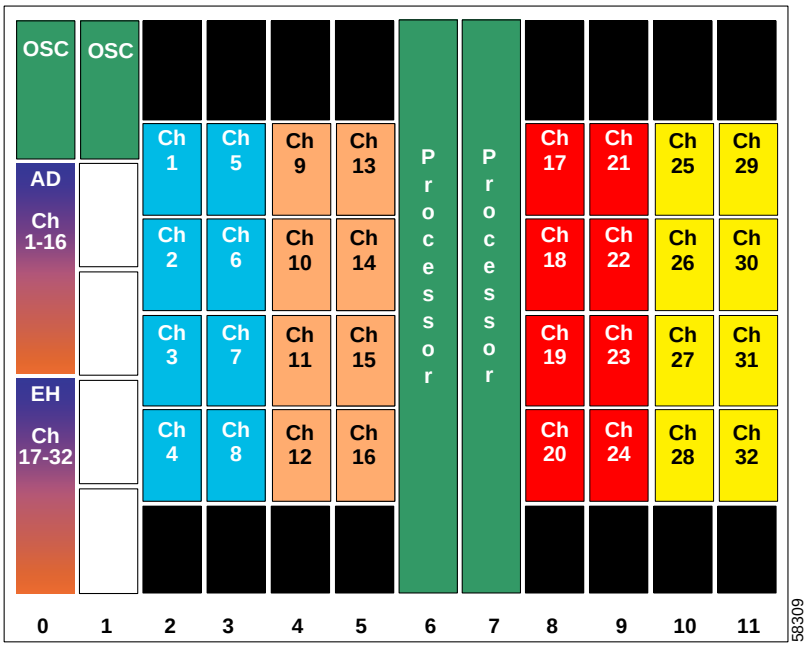
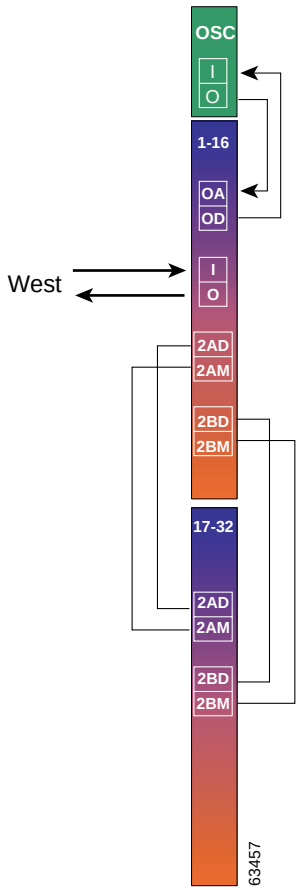


Figure 7-8 shows how the terminal mux/demux modules are cabled for the 32-channel unprotected point-to-point configuration.

Figure 7-8 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 filterband 0/0/0 filtergroup 0/2/0
Node1(config)# patch filterband 0/0/1 filtergroup 0/2/1
```

Node 2

```
Node2# configure terminal
Node2(config)# patch wave 0 oscfilter 0/0
Node2(config)# patch filterband 0/0/0 filtergroup 0/2/0
Node2(config)# patch filterband 0/0/1 filtergroup 0/2/1
```

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>

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>

Node2# copy system:running-config nvram:startup-config
```

CHAPTER 8

Configuring Ring Topologies

This chapter describes how to configure the Cisco ONS 15540 ESP 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

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.

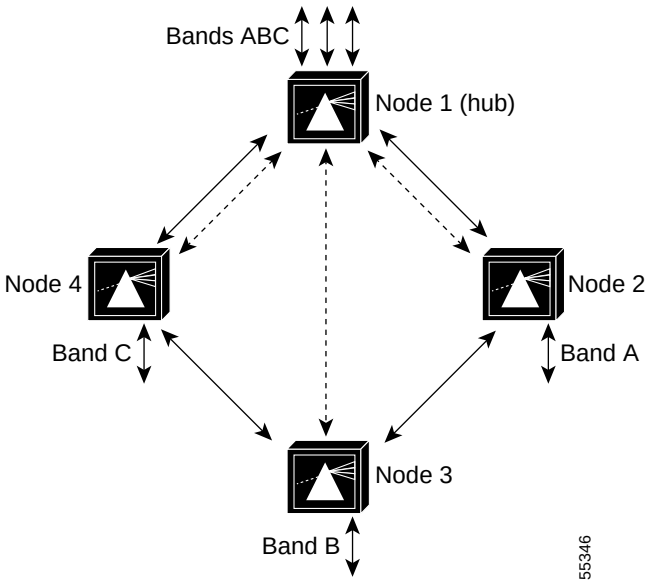
The Cisco ONS 15540 ESP supports hubbed ring and meshed ring topologies.

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 8-1). 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 8-1 Hubbed Ring Topology Example



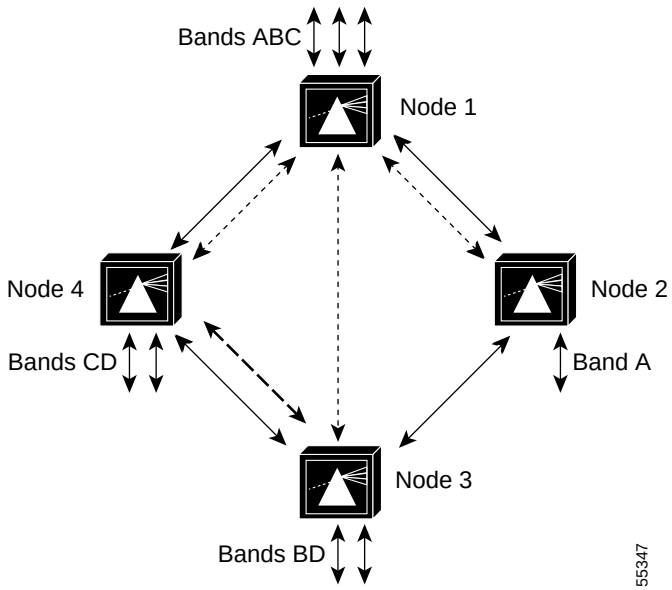
For more information on hubbed ring topologies, refer to the *Introduction to DWDM Technology* document and the *Cisco ONS 15540 ESP Planning and Design Guide*.

Meshed Ring Topologies

A meshed ring is a physical ring that has the characteristics of a mesh. Figure 8-2 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 8-2 Meshed Ring Topology Example

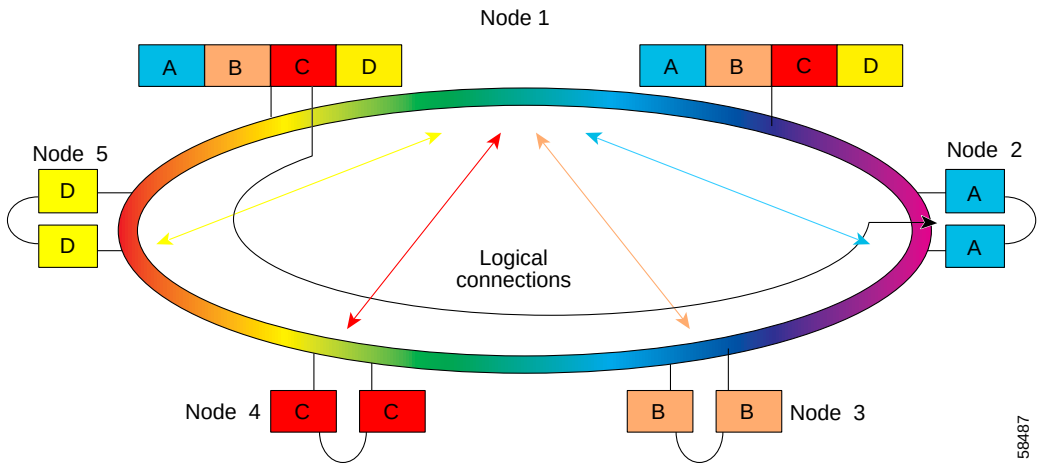


For more information on meshed ring topologies, refer to the *Introduction to DWDM Technology* document and the *Cisco ONS 15540 ESP Planning and Design Guide*.

Configuring a Hubbed Ring with Splitter Protection and OSC

Figure 8-3 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 2.5-Gbps transponder modules carry Gigabit Ethernet traffic.

Figure 8-3 Hubbed Ring Channel Plan



Node 1

Figure 8-4 shows how the modules are installed in the shelf for node 1 in the example network shown in Figure 8-3 on page 8-3. The shelf is populated for the 16-channel splitter protected hub node. Splitter protected line card motherboards are installed in slots 2–5, and the 16-channel mux/demux modules are used in the east and west mux/demux slots.

Figure 8-4 Shelf Configuration for 16-Channel Hub Node in Splitter Protected Hubbed Ring

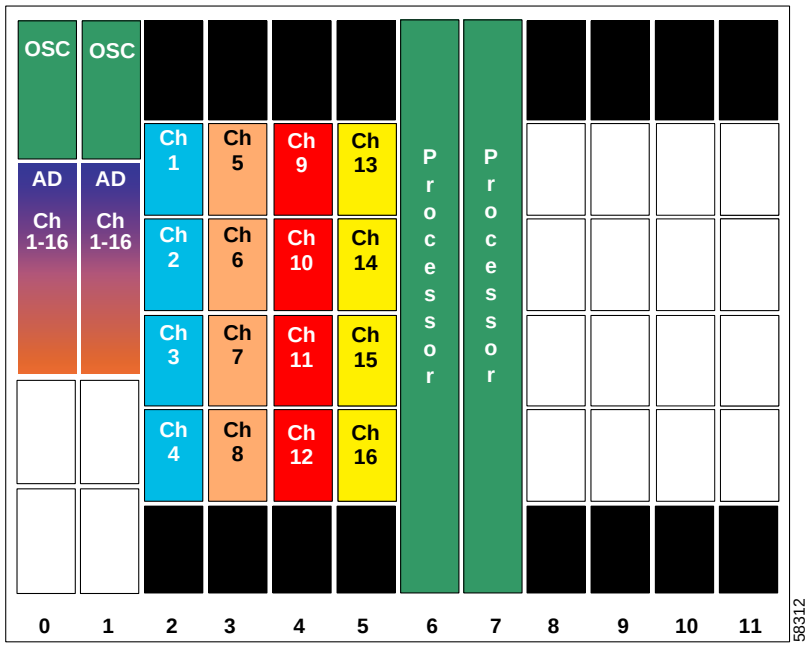
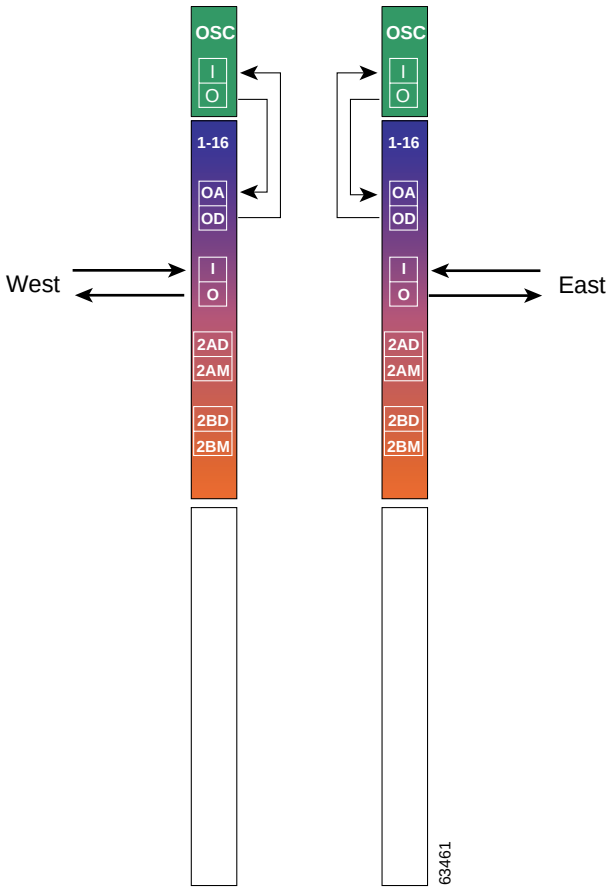


Figure 8-5 shows how the 16-channel mux/demux modules are cabled for the hub node in the splitter protected hubbed ring shown in Figure 8-3 on page 8-3.

Figure 8-5 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 1/0
```

Transparent Interfaces

```
Node1(config)# interface transparent 2/0/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

<Configure the remaining transparent interfaces in the shelf>
```

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 channe110
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 8-6 shows the shelf configuration for node 2 in the example hubbed ring network shown in Figure 8-3 on page 8-3. A splitter protected line card motherboard is used in slot 2, and 4-channel mux/demux modules are used in subcard 0 of the east and west mux/demux slots.

Figure 8-6 Shelf Configuration for Node 2 in Splitter Protected Hubbed Ring

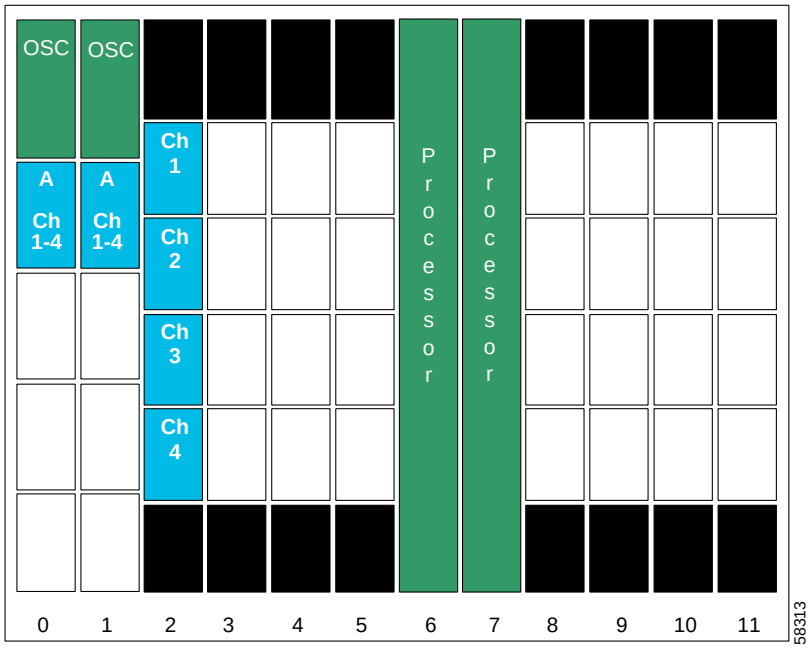
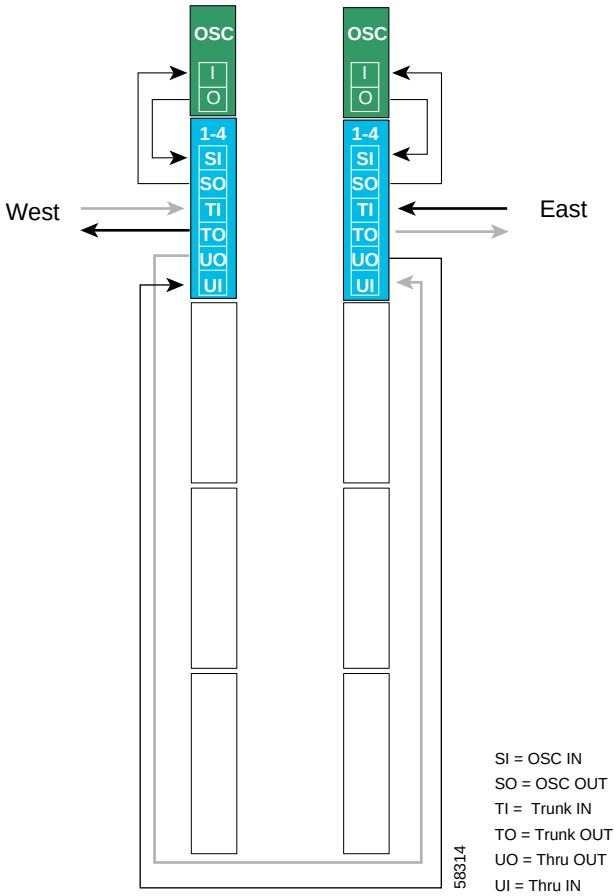


Figure 8-7 shows how the 4-channel mux/demux modules are cabled for node 2 in the splitter protected hubbed ring shown in Figure 8-3 on page 8-3.

Figure 8-7 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
```

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

<Configure the remaining transparent interfaces in the slot>
```

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 8-8 shows the shelf configuration for node 3 in the example hubbed ring network shown in Figure 8-3 on page 8-3. A splitter protected line card motherboard is used in slot 5, and 4-channel mux/demux modules are used in subcard 1 of the east and west mux/demux slots.

Figure 8-8 Shelf Configuration for Node 3 in Splitter Protected Hubbed Ring

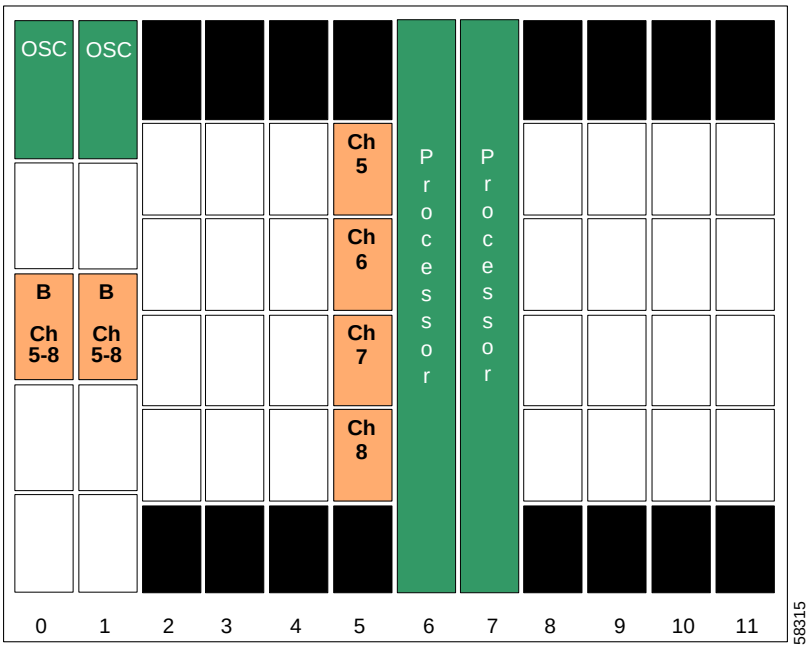
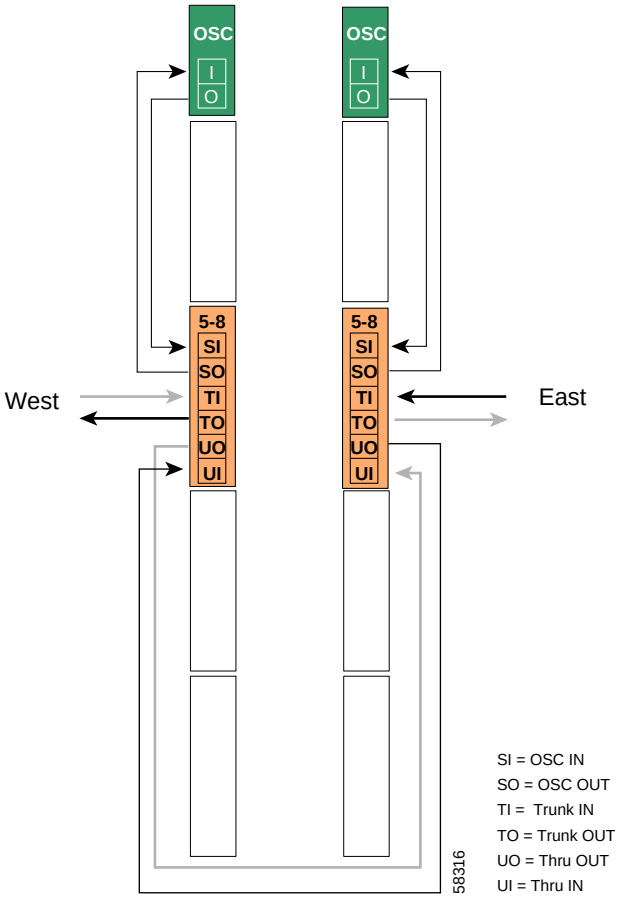


Figure 8-9 shows how the 4-channel mux/demux modules are cabled for node 3 in the splitter protected hubbed ring network shown in Figure 8-3 on page 8-3.

Figure 8-9 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
```

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

<Configure the remaining transparent interfaces in the slot>
```

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 8-10 shows the shelf configuration for node 4 in the hubbed ring network shown in Figure 8-3 on page 8-3. A splitter protected line card motherboard is used in slot 8, and 4-channel mux/demux modules are used in subcard 2 of the east and west mux/demux slots.

Figure 8-10 Shelf Configuration for Node 4 in Splitter Protected Hubbed Ring

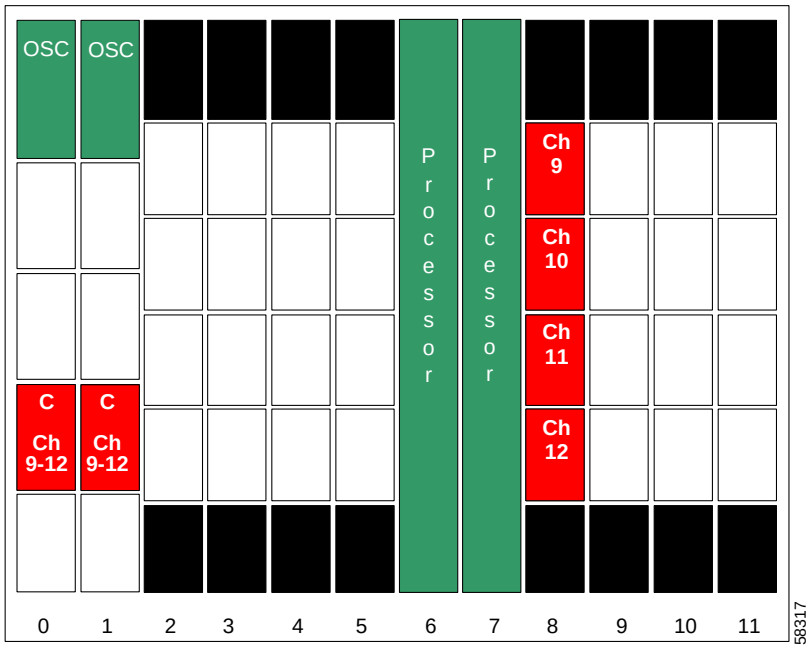
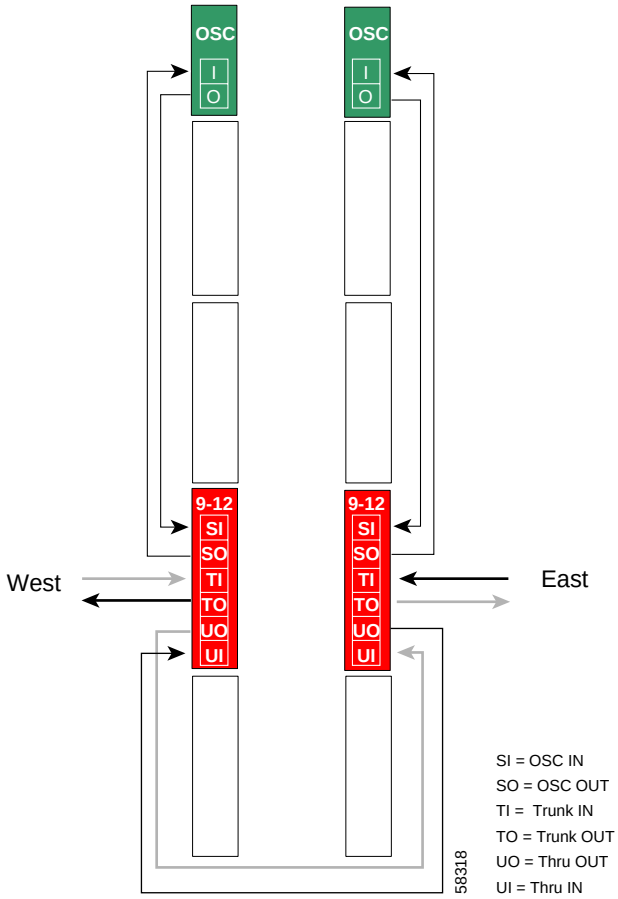


Figure 8-11 shows how the 4-channel mux/demux modules are cabled for node 4 in the splitter protected hubbed ring network shown in Figure 8-3 on page 8-3.

Figure 8-11 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
```

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

<Configure the remaining transparent interfaces in the slot>
```

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 8-12 shows the shelf configuration for node 5 in the example network shown in Figure 8-3 on page 8-3. A splitter protected line card motherboard is used in slot 11, and 4-channel mux/demux modules are used in subcard 3 of the east and west mux/demux slots.

Figure 8-12 Shelf Configuration for Node 5 in Splitter Protected Hubbed Ring

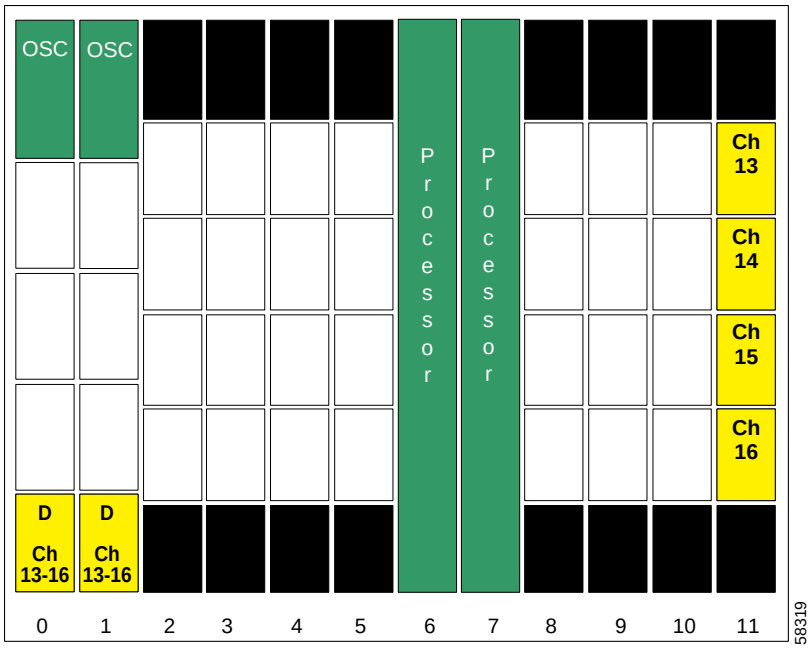
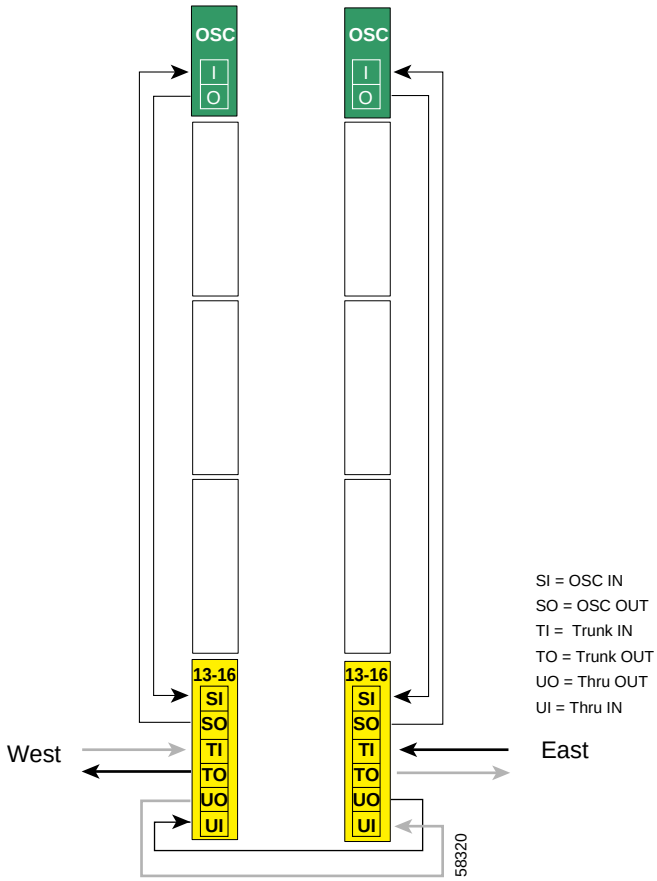


Figure 8-13 shows how the 4-channel mux/demux modules are cabled for node 5 in the example network shown in Figure 8-3 on page 8-3.

Figure 8-13 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
```

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

<Configure the remaining transparent interfaces in the slot>
```

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 8-3 on page 8-3.

Note For information about configuring nodes with more than 16 channels and line card protection, see Chapter 6, “Configuring Dual Shelf Nodes.”

Node 1

Figure 8-14 shows the shelf configuration for the hub node in the hubbed ring example shown in Figure 8-3 on page 8-3. The line card motherboards in slots 2–5 are west motherboards, corresponding to the 16-channel mux/demux module in the west mux/demux slot; the line card motherboards in slots 8–11 are east motherboards, corresponding to the 16-channel mux/demux module in the east mux/demux slot.

Figure 8-14 Shelf Configuration for Hub Node in Line Card Protected Hubbed Ring

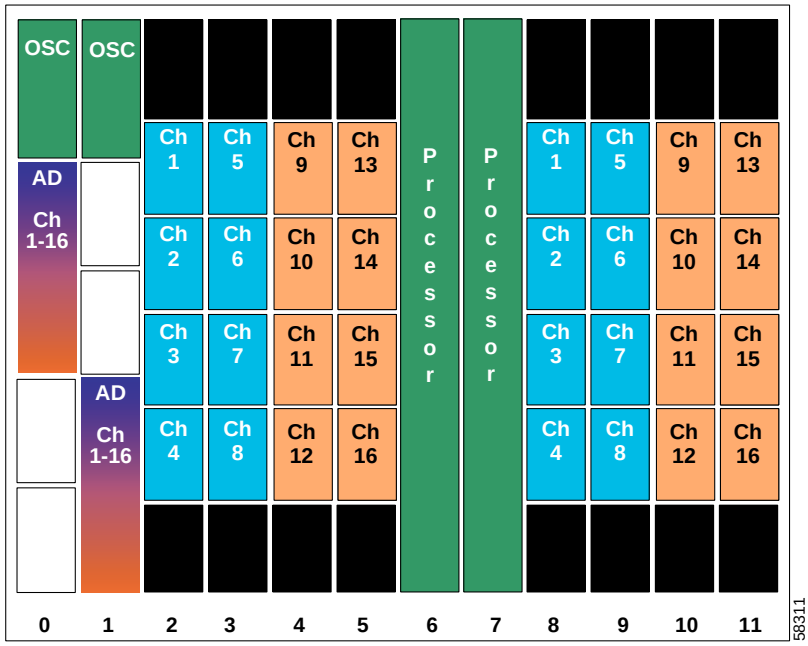
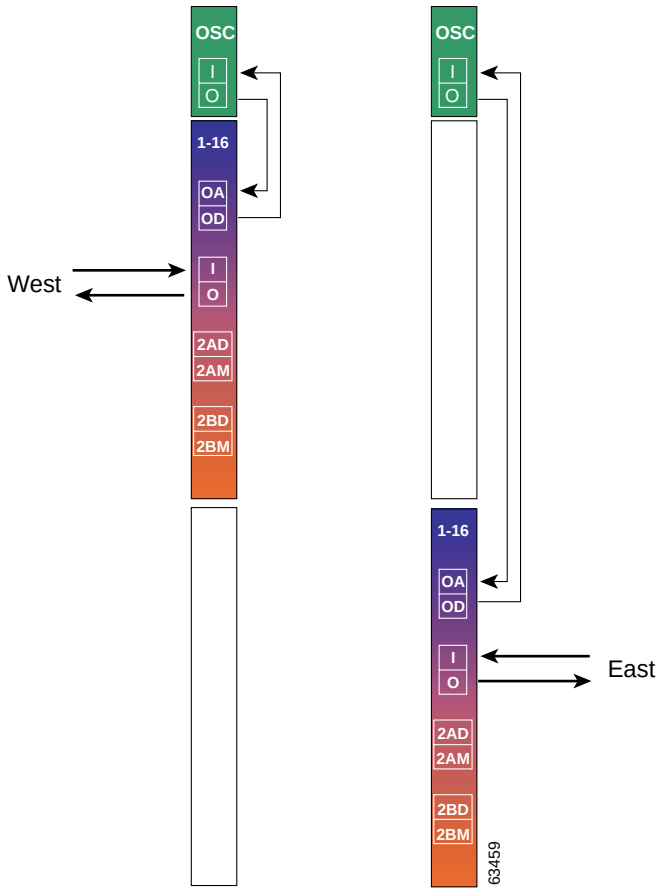


Figure 8-15 shows how the 16-channel mux/demux modules are cabled for node 1 in the hub node in the line card protected hubbed ring shown in Figure 8-3 on page 8-3.

Figure 8-15 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 1/2
```

Transparent Interfaces

```
Node1(config)# interface transparent 2/0/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit

<Configure the remaining transparent interfaces in the shelf>
```

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
```

Node 2

Figure 8-16 shows the shelf configuration for node 2 in the line card protected hubbed ring shown in Figure 8-3 on page 8-3. Slot 2 uses a west line card motherboard, corresponding to the add/drop mux/demux module in the west mux/demux slot; slot 4 uses an east line card motherboard, corresponding to the add/drop mux/demux module in the east mux/demux slot.

Figure 8-16 Shelf Configuration for Node 2 in Line Card Protected Hubbed Ring

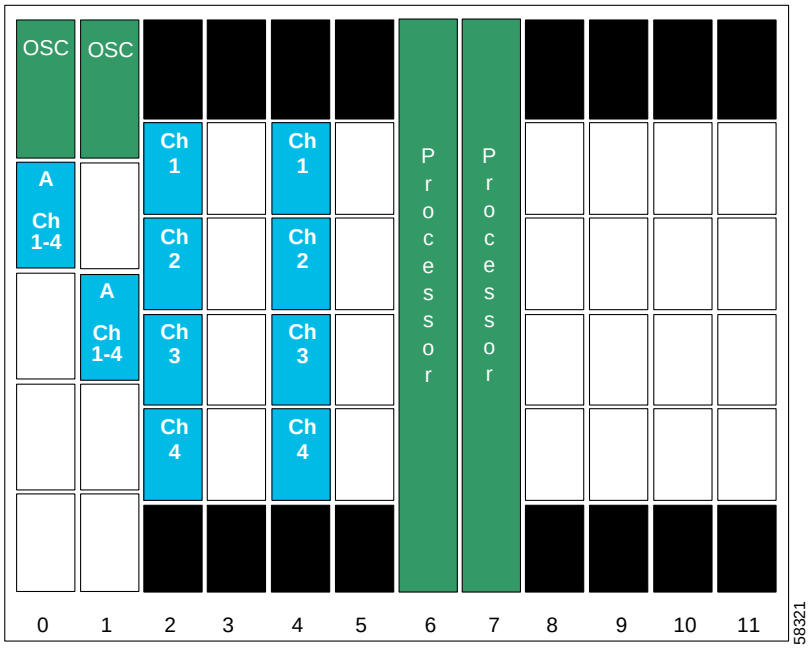
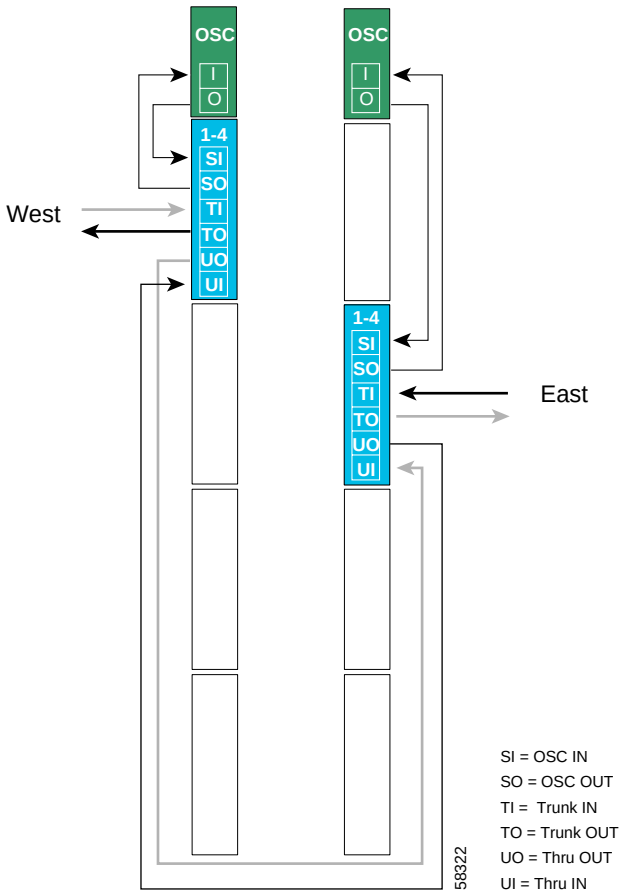


Figure 8-17 shows how the 4-channel mux/demux modules are cabled for node 2 in the line card protected hubbed ring shown in Figure 8-3 on page 8-3.

Figure 8-17 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
```

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

<Configure the remaining transparent interfaces in the slot>
```

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

<Configure the remaining transparent interfaces in the slot>
```

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 8-18 shows the shelf configuration for node 3 in the line card protected hubbed ring shown in Figure 8-3 on page 8-3. Slot 3 uses an east line card motherboard, corresponding to the add/drop mux/demux module in the east mux/demux slot; slot 5 uses a west line card motherboard, corresponding to the add/drop mux/demux module in the west mux/demux slot.

Figure 8-18 Shelf Configuration for Node 3 in Line Card Protected Hubbed Ring

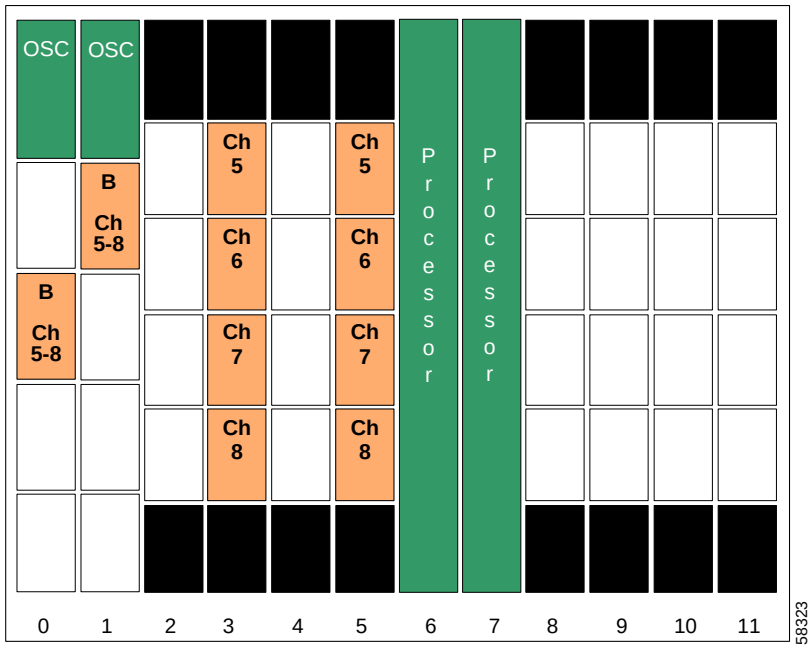
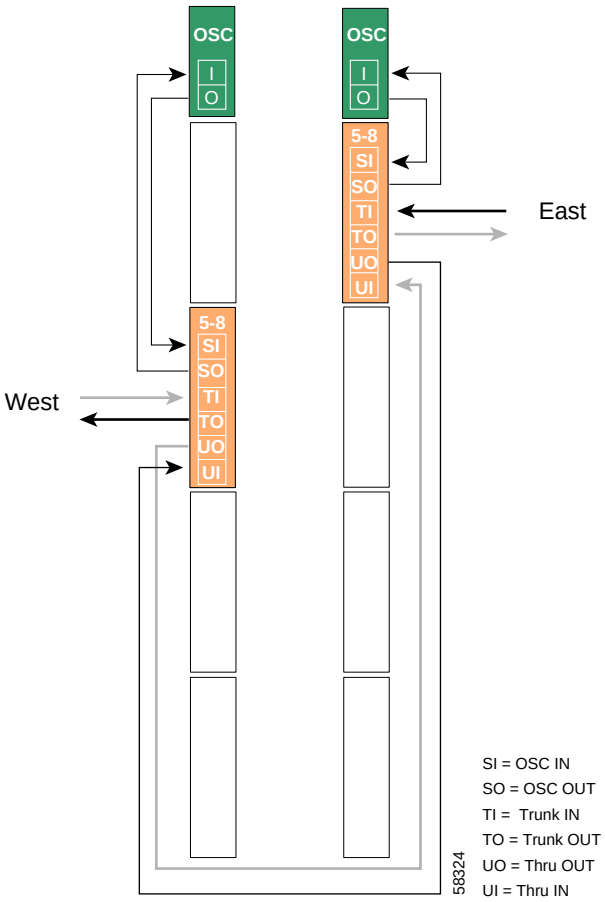


Figure 8-19 shows how the 4-channel mux/demux modules are cabled for node 3 in the line card protected hubbed ring shown in Figure 8-3 on page 8-3.

Figure 8-19 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
```

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

<Configure the remaining transparent interfaces in the slot>
```

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

<Configure the remaining transparent interfaces in the slot>
```

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 8-20 shows the shelf configuration for node 4 in the line card protected hubbed ring shown in Figure 8-3 on page 8-3. Slot 8 uses a west line card motherboard, corresponding to the add/drop mux/demux module in the west mux/demux slot; slot 10 uses an east line card motherboard, corresponding to the add/drop mux/demux module in the east mux/demux slot.

Figure 8-20 Module Installation Configuration for Node 4

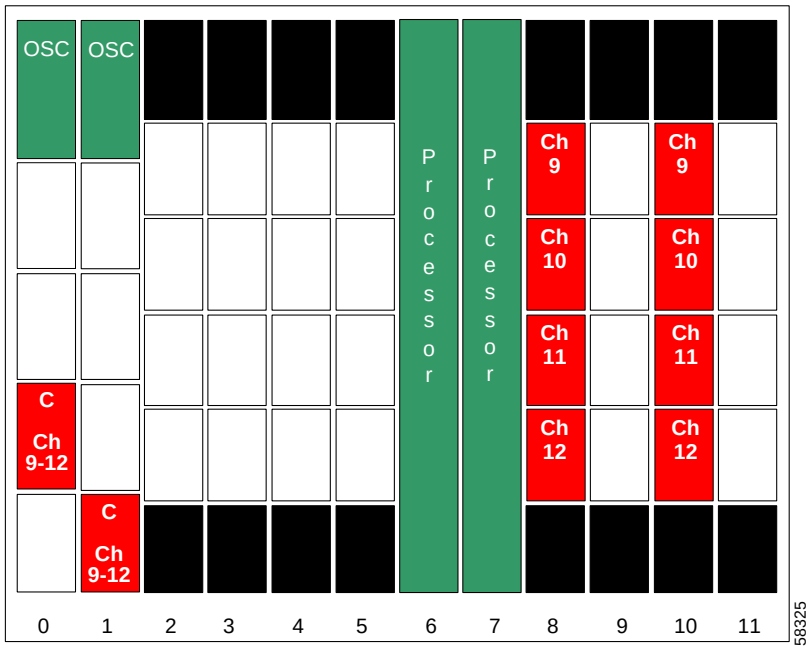
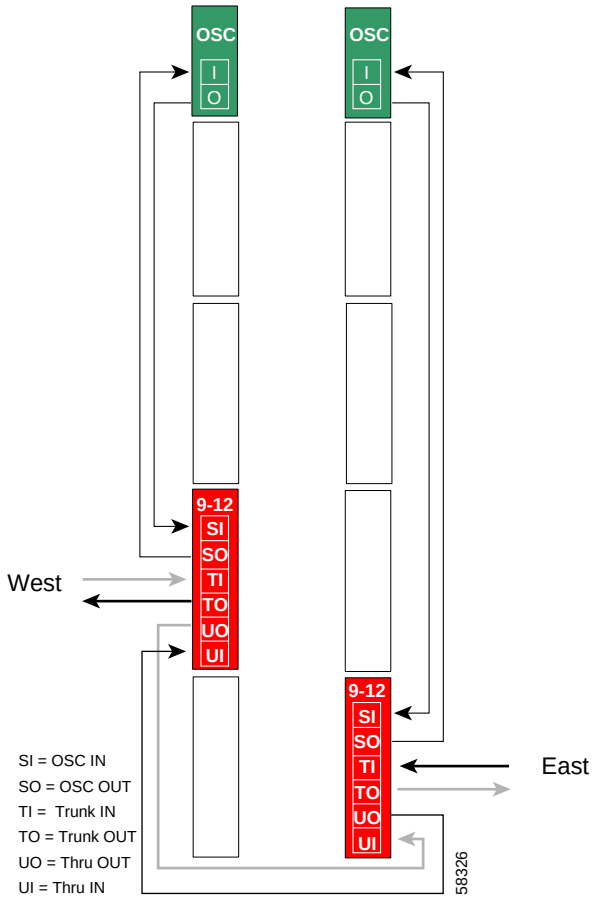


Figure 8-21 shows how the 4-channel mux/demux modules are cabled for node 4 in the line card protected hubbed ring shown in Figure 8-3 on page 8-3.

Figure 8-21 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
```

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

<Configure the remaining transparent interfaces in the slot>
```

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

<Configure the remaining transparent interfaces in the slot>
```

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 8-22 shows the shelf configuration for node 5 in the line card protected hubbed ring shown in Figure 8-3 on page 8-3. Slot 9 uses an east line card motherboard, corresponding to the add/drop mux/demux module in the east mux/demux slot; slot 11 uses a west line card motherboard, corresponding to the add/drop mux/demux module in the west mux/demux slot.

Figure 8-22 Shelf Configuration for Node 5 in Line Card Protected Hubbed Ring

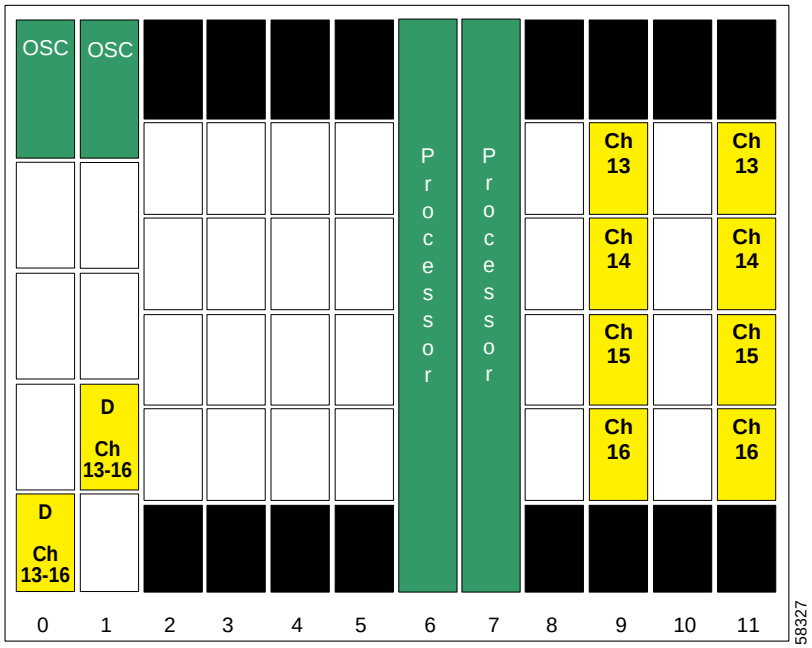
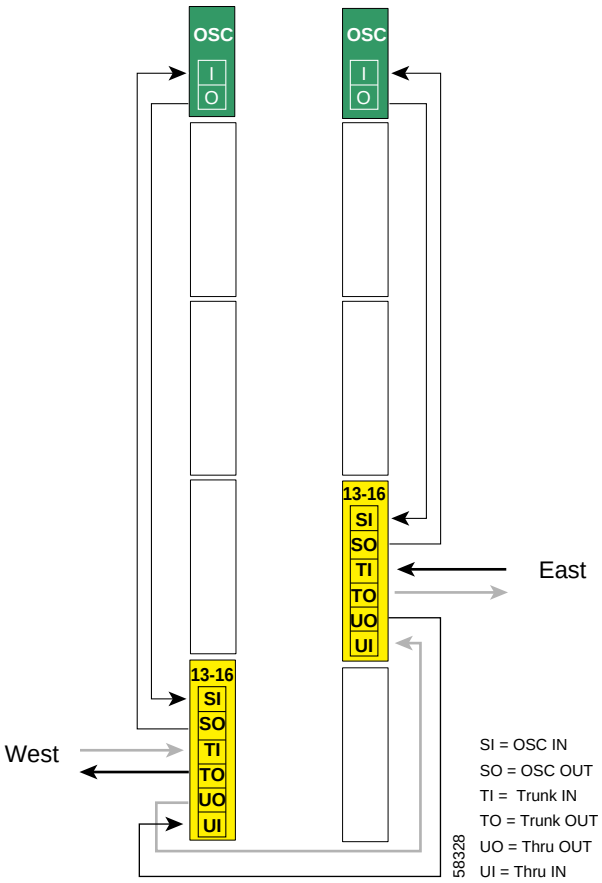


Figure 8-23 shows how the 4-channel mux/demux modules are cabled for node 5 in the line card protected hubbed ring shown in Figure 8-3 on page 8-3.

Figure 8-23 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
```

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

<Configure the remaining transparent interfaces in the slot>
```

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

<Configure the remaining transparent interfaces in the slot>
```

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.

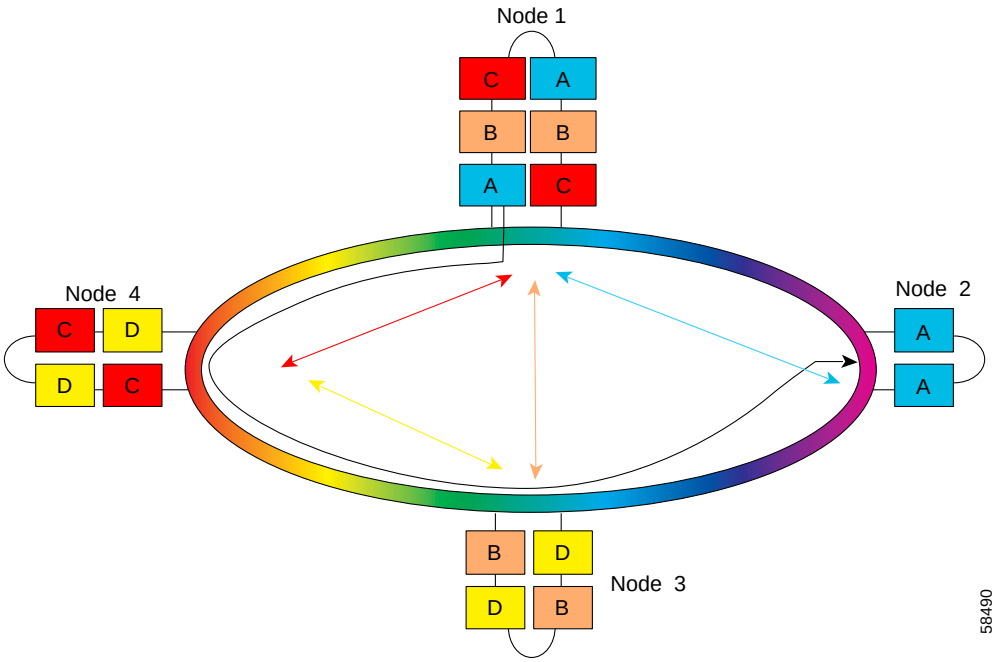
```
Node5(config)# redundancy
Node5(config-red)# associate group channel13
Node5(config-red-aps)# aps working transparent 9/0/0
Node5(config-red-aps)# aps protection transparent 11/0/0
Node5(config-red-aps)# aps y-cable
Node5(config-red-aps)# aps revertive
Node5(config-red-aps)# aps enable
Node5(config-red-aps)# 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 8-24 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 2.5-Gbps transponder modules carry Gigabit Ethernet traffic.

Figure 8-24 Channel Plan for Meshed Ring



Node 1

Figure 8-25 shows the shelf configuration for node 1 in the splitter protected meshed ring shown in Figure 8-24 on page 8-36. Splitter protected line card motherboards are used to couple the signal to the add/drop mux/demux modules in both west and east mux/demux slots.

Figure 8-25 Shelf Configuration for Node 1 in Splitter Protected Meshed Ring

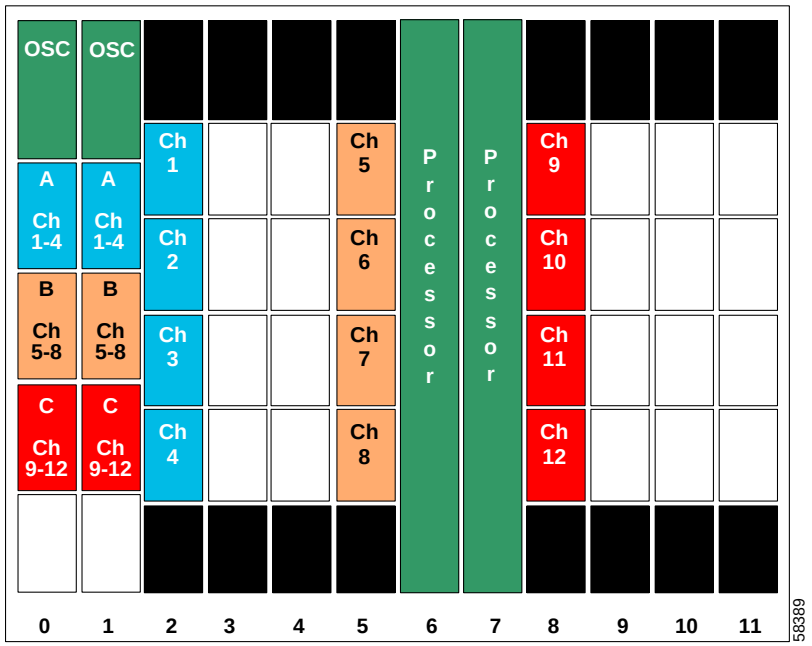
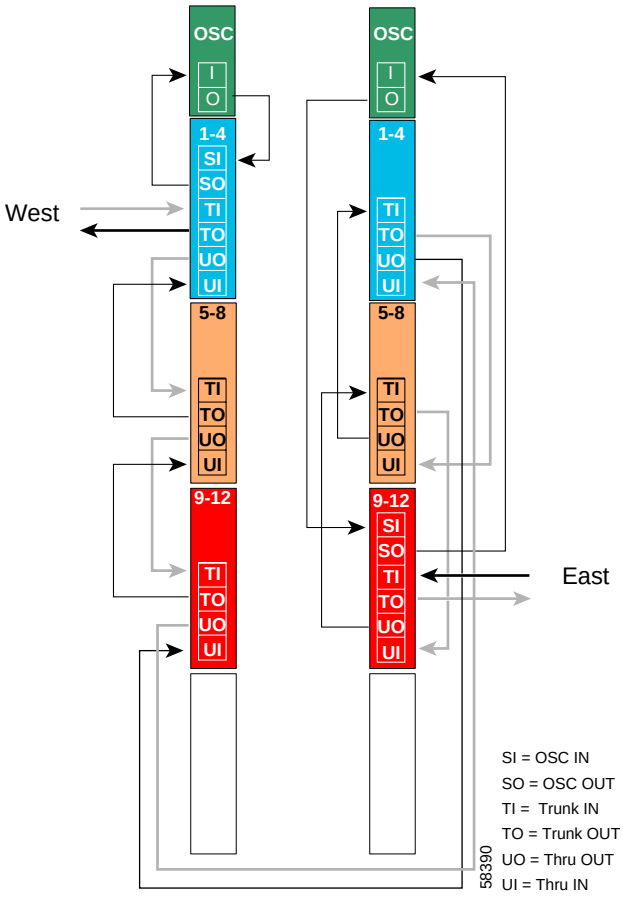


Figure 8-26 shows how the 4-channel mux/demux modules are cabled for node 1 in the splitter protected meshed ring shown in Figure 8-24 on page 8-36.

Figure 8-26 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
```

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
<Configure the remaining transparent interfaces in the slot>
```

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

<Configure the remaining transparent interfaces in the slot>
```

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

<Configure the remaining transparent interfaces in the slot>
```

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 8-27 shows the shelf configuration for node 2 in the splitter protected meshed ring shown in Figure 8-24 on page 8-36. Slot 2 uses the splitter protected line card motherboard, which couples the signal to the add/drop mux/demux modules in both west and east mux/demux slots.

Figure 8-27 Shelf Configuration for Node 2 in Splitter Protected Meshed Ring

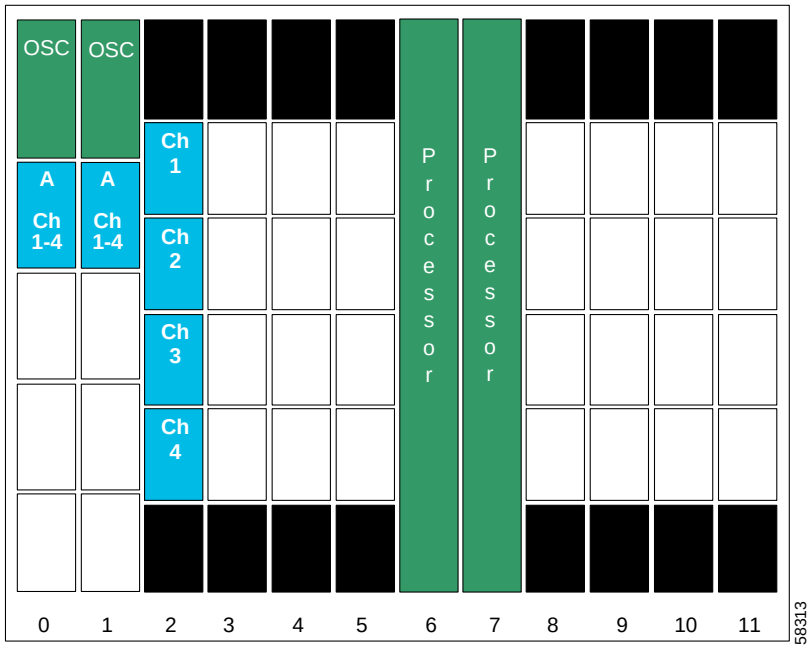
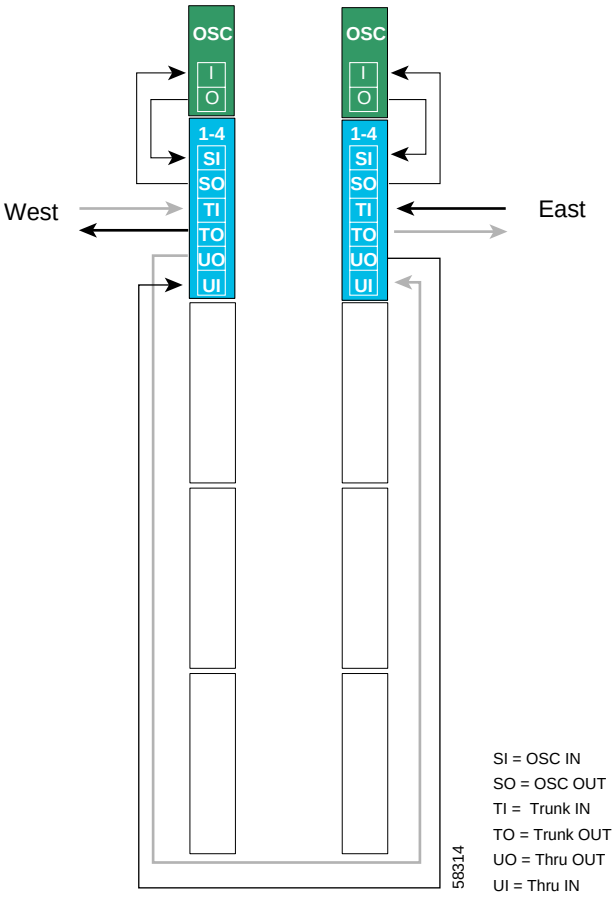


Figure 8-28 shows how the 4-channel mux/demux modules are cabled for node 2 in the splitter protected meshed ring shown in Figure 8-24 on page 8-36.

Figure 8-28 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
```

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

<Configure the remaining transparent interfaces in the slot>
```

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 8-29 shows the shelf configuration for node 3 in the splitter protected meshed ring shown in Figure 8-24 on page 8-36. Slots 5 and 11 use splitter protected line card motherboards, which couple the signal to the add/drop mux/demux modules in both west and east mux/demux slots.

Figure 8-29 Shelf Configuration for Node 3 in Splitter Protected Meshed Ring

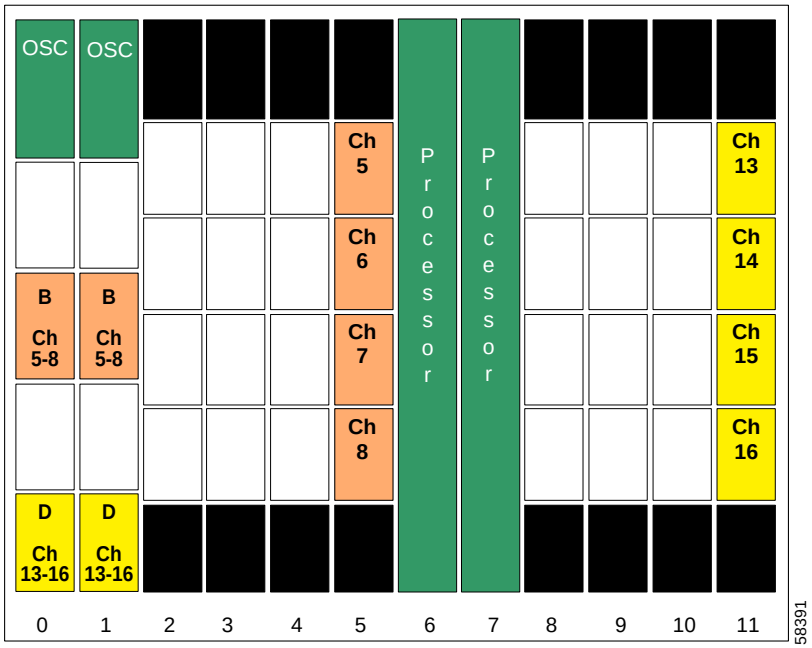
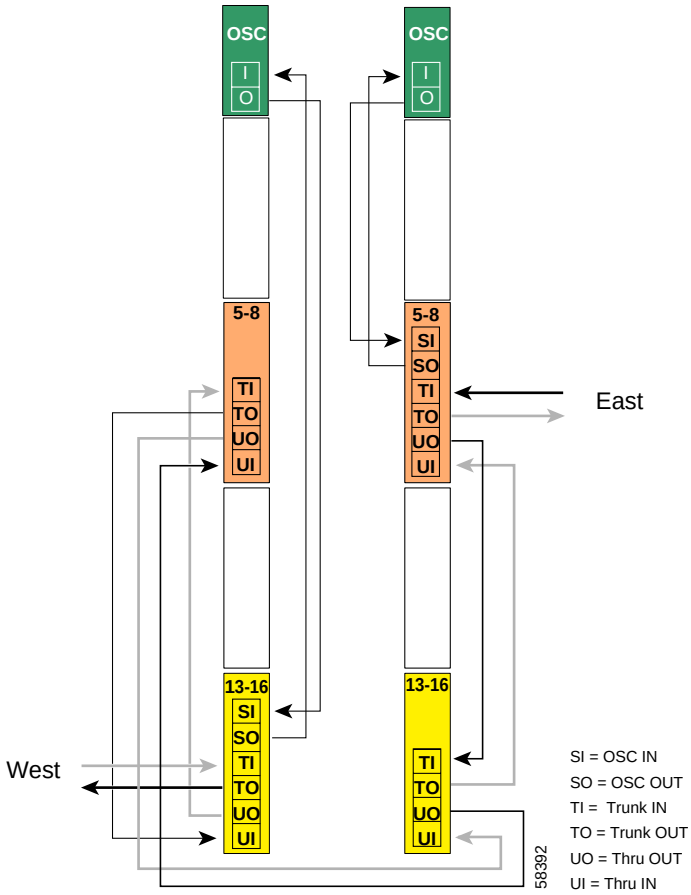


Figure 8-30 shows how the 4-channel mux/demux modules are cabled for node 3 in the splitter protected meshed ring shown in Figure 8-24 on page 8-36.

Figure 8-30 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
```

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

<Configure the remaining transparent interfaces in the slot>
```

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

<Configure the remaining transparent interfaces in the slot>
```

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

Figure 8-31 shows the shelf configuration for node 4 in the splitter protected meshed ring shown in Figure 8-24 on page 8-36. Slots 8 and 11 use the splitter protected line card motherboards, which couple the signal to the add/drop mux/demux modules in both the west and east mux/demux slots.

Figure 8-31 Module Installation Configuration for Node 4

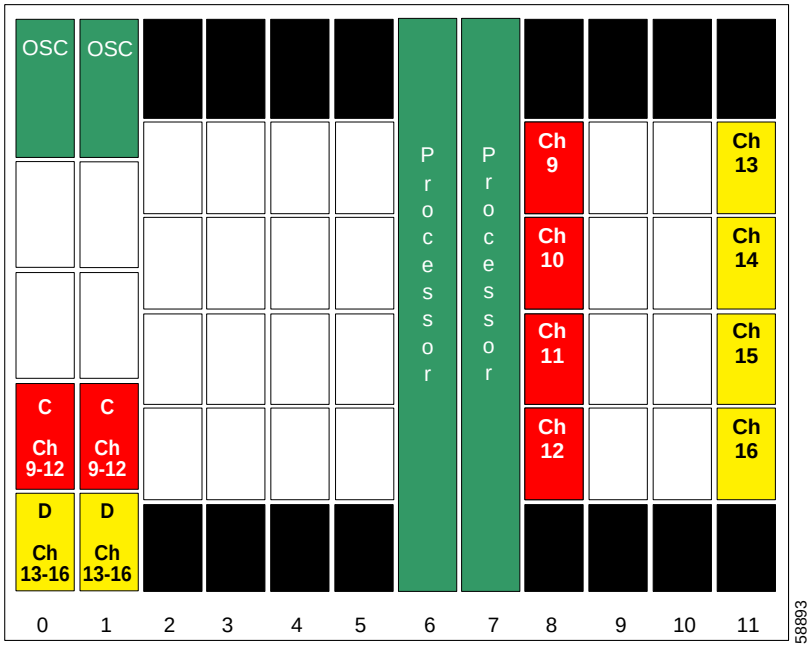
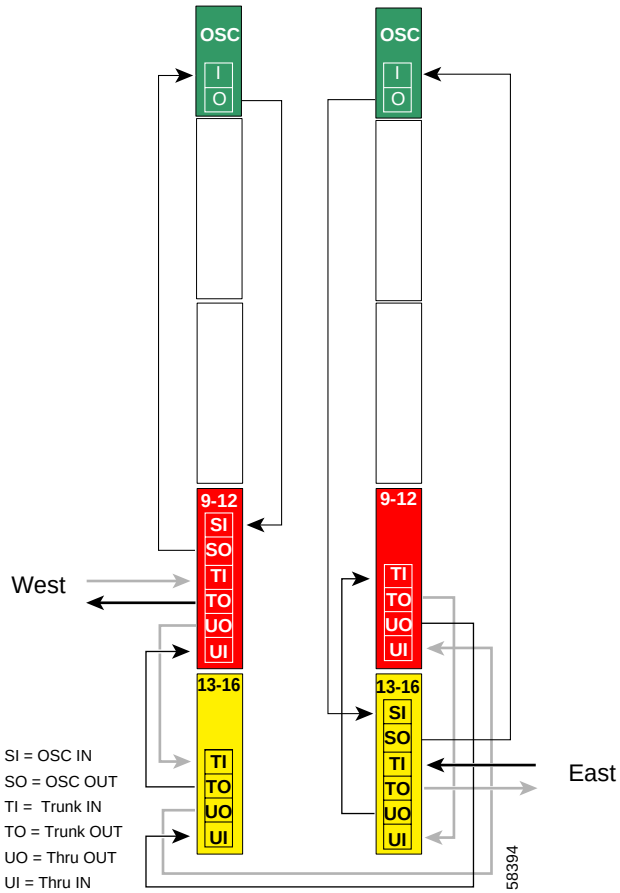


Figure 8-32 shows how the 4-channel mux/demux modules are cabled for node 4 in the splitter protected meshed ring shown in Figure 8-24 on page 8-36.

Figure 8-32 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
```

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

<Configure the remaining transparent interfaces in the slot>
```

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

<Configure the remaining transparent interfaces in the slot>
```

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
```

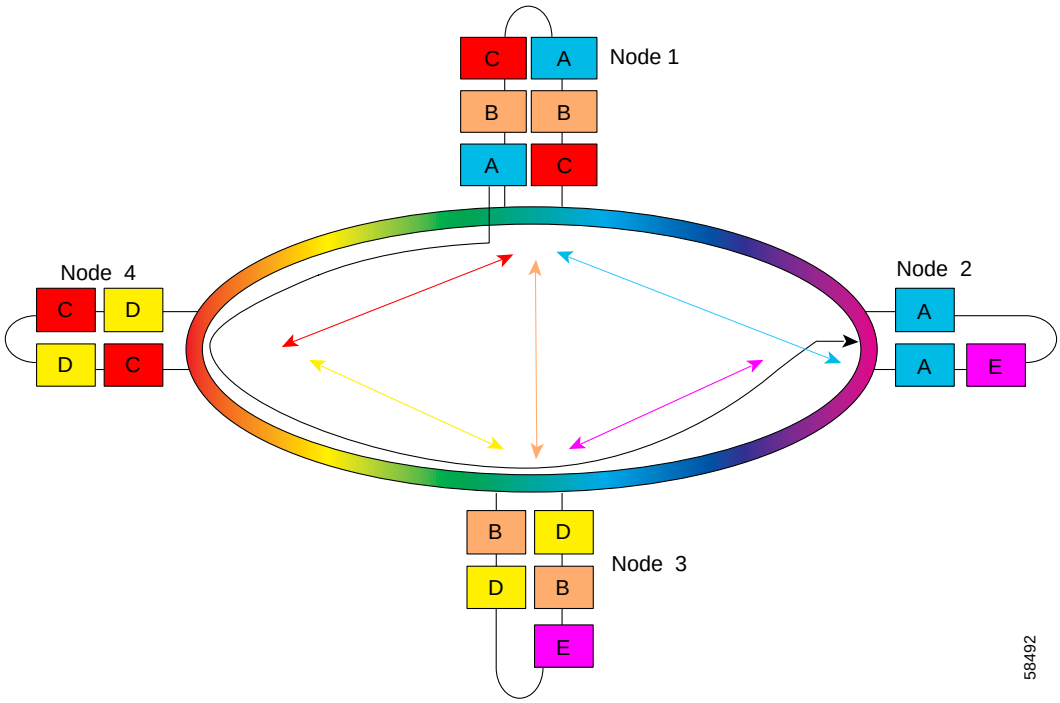
```
Node4(config-red-aps)# aps enable
Node4(config-red-aps)# end

Node4# copy system:running-config nvram:startup-config
```

Configuring a Splitter Protected Meshed Ring with Unprotected Channels and OSC

Figure 8-33 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 2.5-Gbps transponder modules carry Gigabit Ethernet traffic.

Figure 8-33 Overview of Meshed Ring Topology with Splitter Protection



Node 1

The configuration for node 1 is the same as described in the “Node 1” section on page 8-37.

Node 2

Figure 8-34 shows the shelf configuration for node 2 in the splitter protected meshed ring with unprotected channels shown in Figure 8-33 on page 8-50. Slot 2 uses the splitter protected line card motherboard, which couples the signal to the add/drop mux/demux modules in subcard 0 of both west and east mux/demux slots. Slot 4, which supports the unprotected channels, uses an east line card motherboard.

Figure 8-34 Shelf Configuration for Node 2 in Splitter Protected Meshed Ring with Unprotected Channels

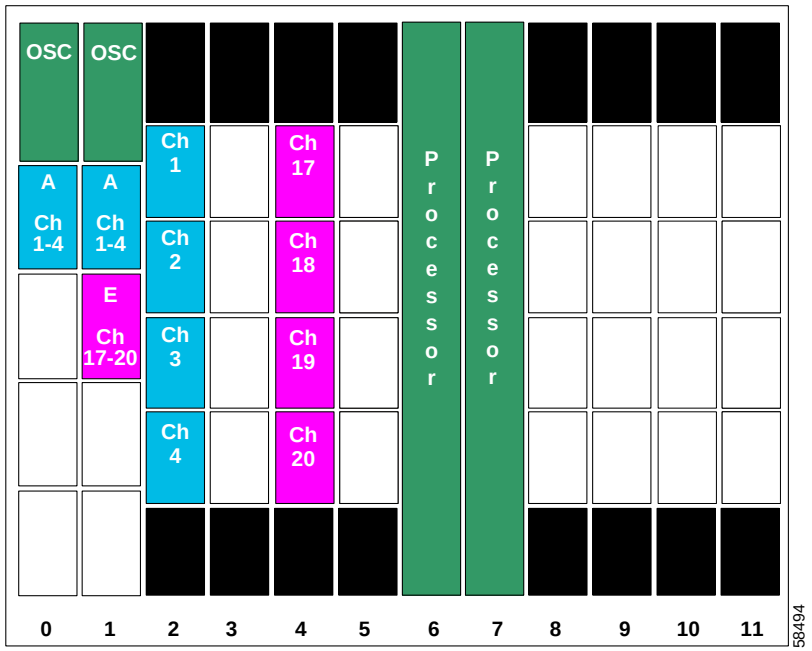
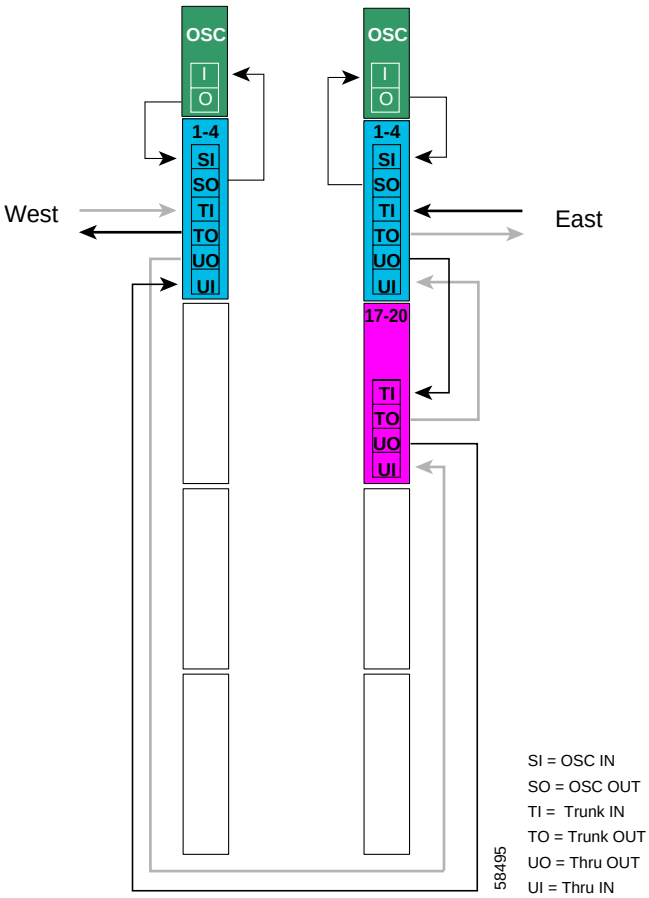


Figure 8-35 shows how the 4-channel mux/demux modules are cabled for node 2 in the splitter protected meshed ring with unprotected channel shown in Figure 8-33 on page 8-50.

Figure 8-35 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
```

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

<Configure the remaining transparent interfaces in the slot>
```

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

<Configure the remaining transparent interfaces in the slot>
```

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 8-36 shows the shelf configuration for node 3 in the splitter protected meshed ring with unprotected channels shown in Figure 8-33 on page 8-50. Slot 5 and slot 11 use splitter protected line card motherboards, which couple the signal to the add/drop mux/demux modules in subcard 1 and subcard 3, respectively, of both west and east mux/demux slots. Slot 8, which supports the unprotected channels, uses a west line card motherboard.

Figure 8-36 Shelf Configuration for Node 3 in Splitter Protected Meshed Ring with Unprotected Channels

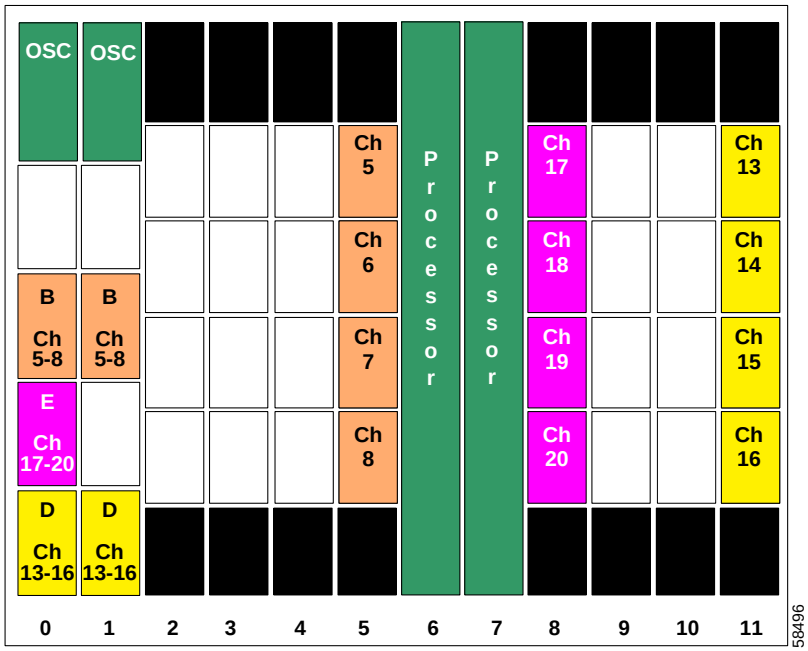
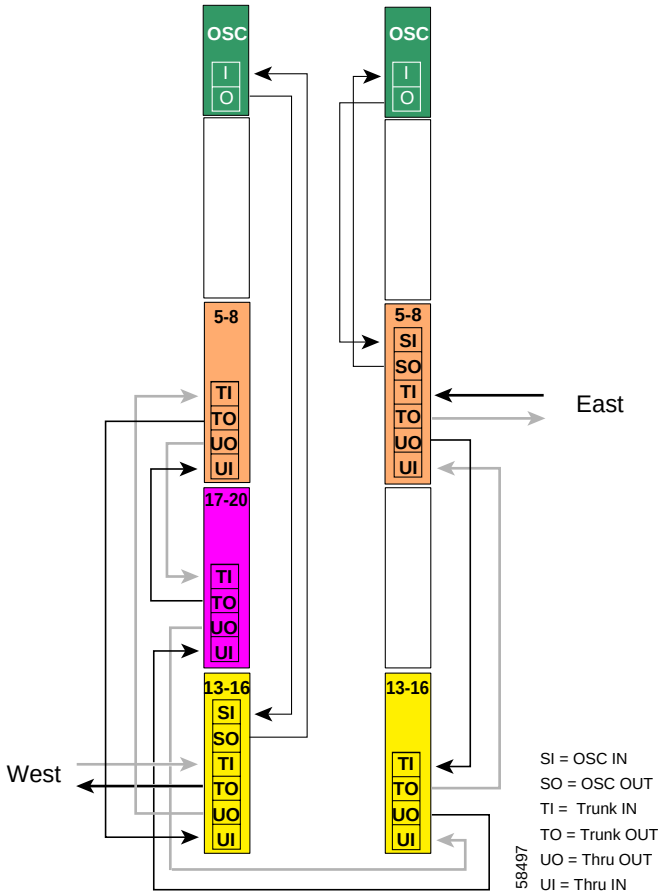


Figure 8-37 shows how the 4-channel mux/demux modules are cabled for node 3 in the splitter protected meshed ring with unprotected channels shown in Figure 8-33 on page 8-50.

Figure 8-37 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
```

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

<Configure the remaining transparent interfaces in the slot>
```

Transparent Interfaces in Slot 8

```
Node3(config)# interface transparent 8/0/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit

<Configure the remaining transparent interfaces in the slot>
```

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

<Configure the remaining transparent interfaces in the slot>
```

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 8-47.

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 8-24 on page 8-36.

Node 1

Figure 8-38 shows the shelf configuration for node 1 using line card protection in the example meshed ring shown in Figure 8-24 on page 8-36. Slots 2, 5, and 8 use west line card motherboards, corresponding to the add/drop mux/demux modules in the west mux/demux slot; slots 3, 4, and 10 use east line card motherboards, corresponding to the add/drop mux/demux modules in the east mux/demux slot.

Figure 8-38 Shelf Configuration for Node 1 in Line Card Protected Meshed Ring

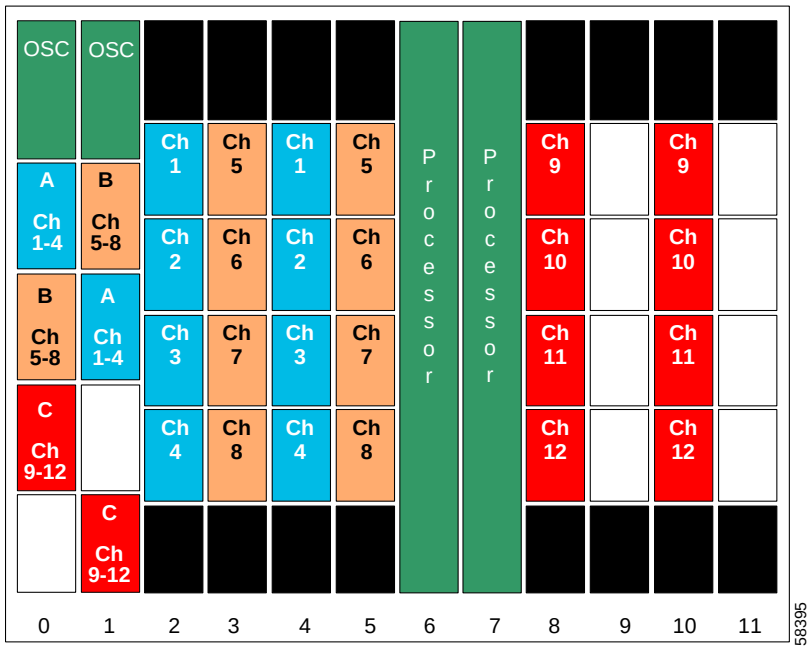
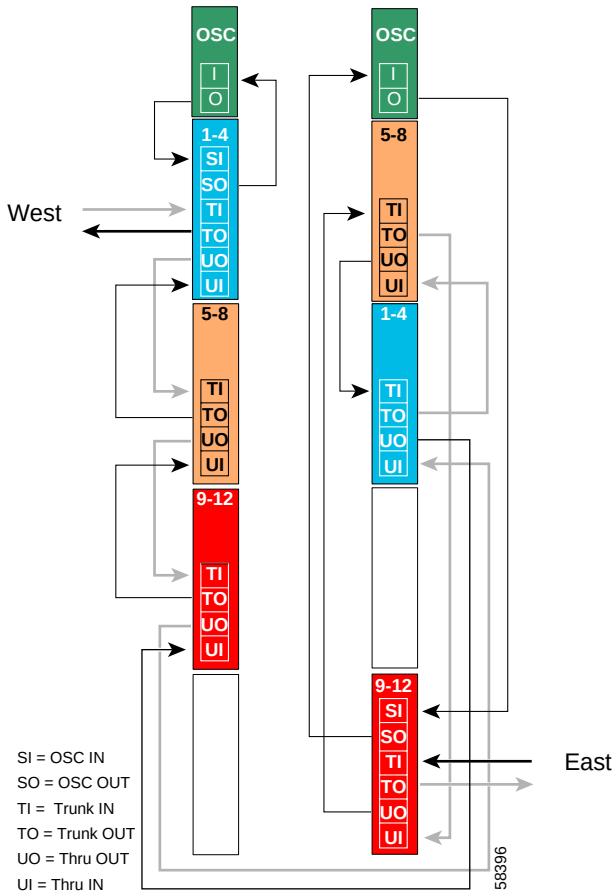


Figure 8-39 shows how the 4-channel mux/demux modules are cabled for node 1 in the line card protected meshed ring shown in Figure 8-24 on page 8-36.

Figure 8-39 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
```

Transparent Interfaces

```
Node1(config)# interface transparent 2/0/0
Node1(config-if)# encapsulation gigabitethernet
Node1(config-if)# monitor enable
Node1(config-if)# exit
```

```
<Configure the remaining transparent interfaces in the shelf>
```

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 8-40 shows the shelf configuration for node 2 in the line card protected meshed ring shown in Figure 8-24 on page 8-36. Slot 2 uses the west line card motherboard, corresponding to the add/drop mux/demux module in the west mux/demux slot; slot 4 uses the east line card motherboard, corresponding to the add/drop mux/demux module in the east mux/demux slot.

Figure 8-40 Shelf Configuration for Node 2 in Line Card Protected Meshed Ring

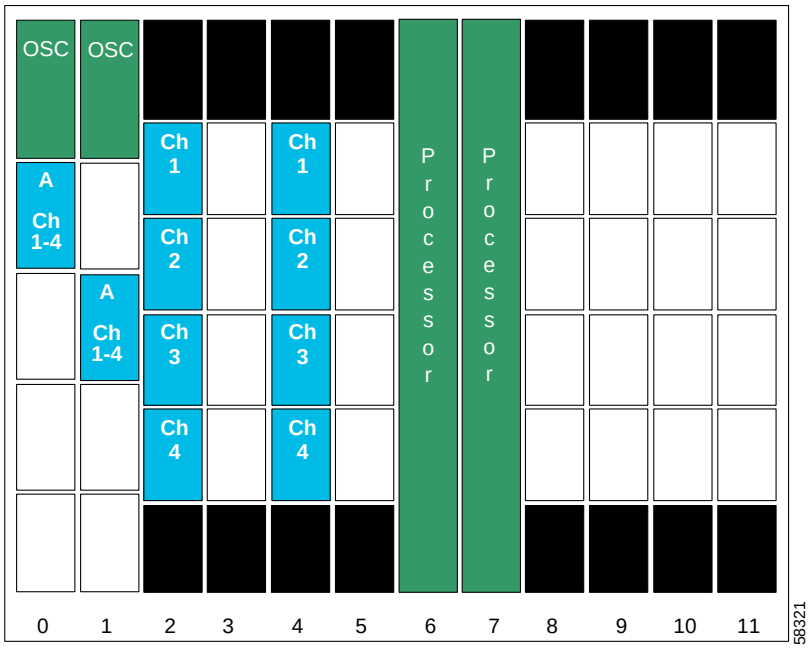
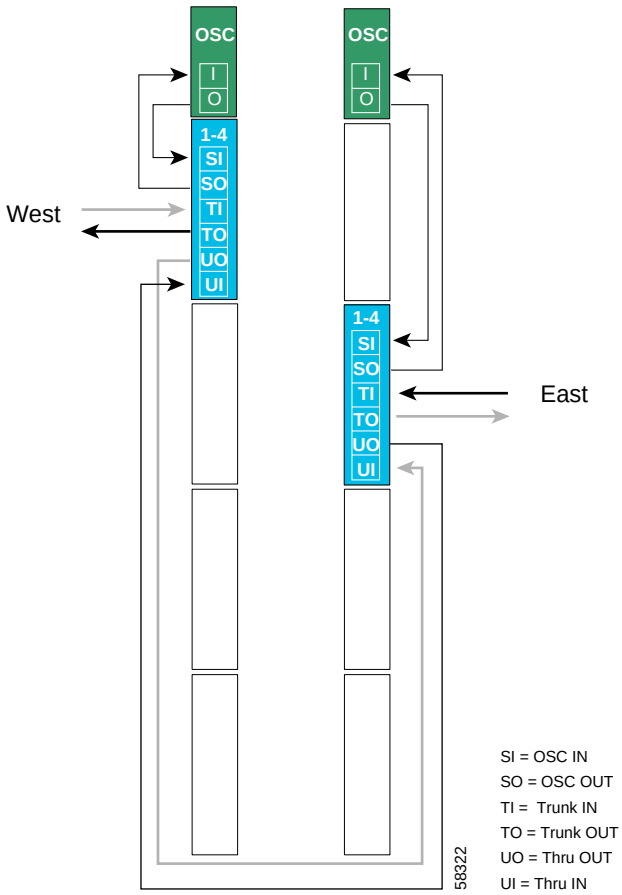


Figure 8-41 shows how the 4-channel mux/demux modules are cabled for node 2 in the line card protected meshed ring shown in Figure 8-24 on page 8-36.

Figure 8-41 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
```

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

<Configure the remaining transparent interfaces in the slot>
```

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

<Configure the remaining transparent interfaces in the slot>
```

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 8-42 shows the shelf configuration for node 3 in the line card protected meshed ring shown in Figure 8-24 on page 8-36. Slots 5 and 11 use the west line card motherboards, corresponding to the add/drop mux/demux modules in the west mux/demux slot; slots 3 and 9 use the east line card motherboards, corresponding to the add/drop mux/demux modules in the east mux/demux slot.

Figure 8-42 Shelf Configuration for Node 3 in Line Card Protected Meshed Ring

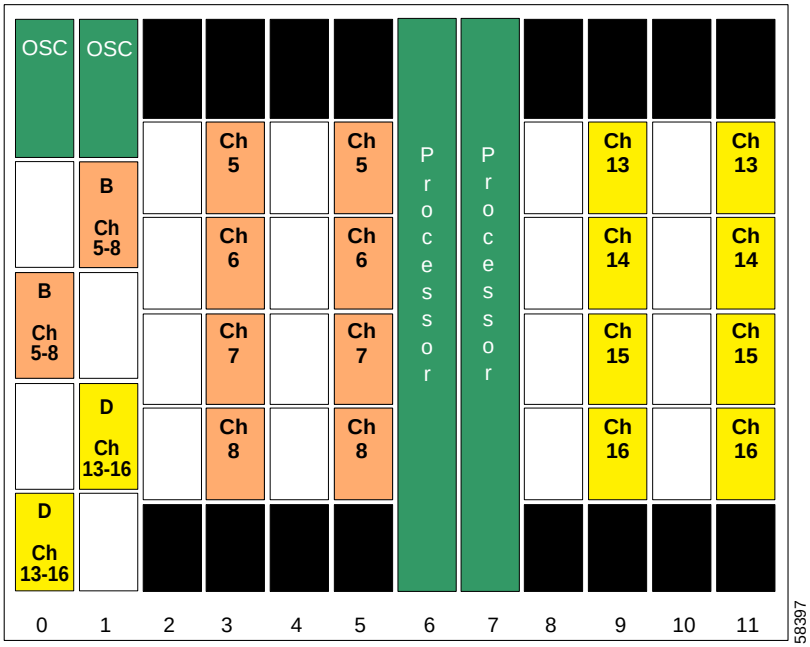
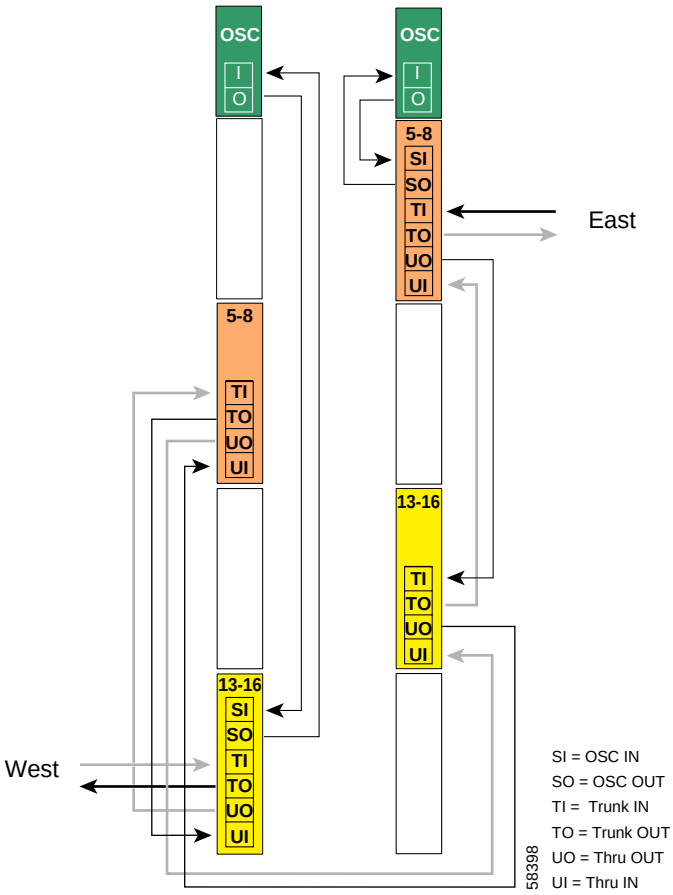


Figure 8-43 shows how the 4-channel mux/demux modules are cabled for the line card protected meshed ring shown in Figure 8-24 on page 8-36.

Figure 8-43 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
```

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

<Configure the remaining transparent interfaces in the slot>
```

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

<Configure the remaining transparent interfaces in the slot>
```

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

<Configure the remaining transparent interfaces in the slot>
```

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

<Configure the remaining transparent interfaces in the slot>
```

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 8-44 shows the shelf configuration for node 4 in the line card protected meshed ring shown in Figure 8-24 on page 8-36. Slots 8 and 11 use the west line card motherboards, corresponding to the add/drop mux/demux modules in the west mux/demux slots; slots 9 and 10 use the east line card motherboards, corresponding to the add/drop mux/demux modules in the east mux/demux slots.

Figure 8-44 Shelf Configuration for Node 4 in Line Card Protected Meshed Ring

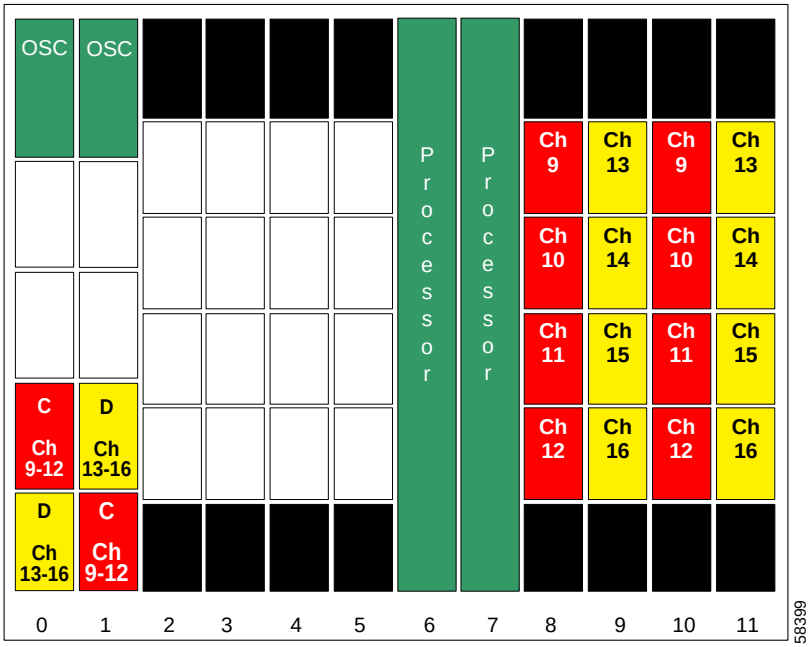
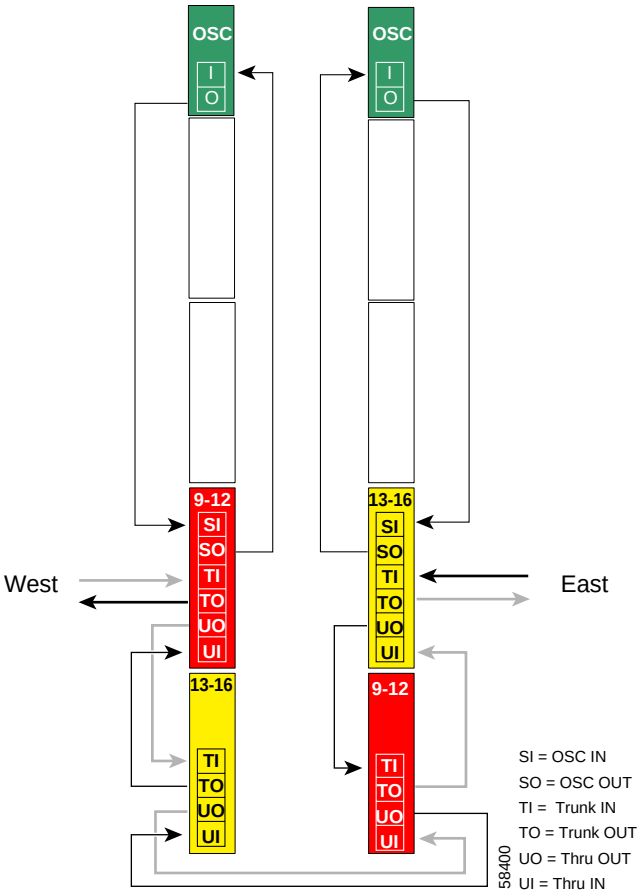


Figure 8-45 shows how the 4-channel mux/demux modules are cabled for node 4 in the line card protected meshed ring shown in Figure 8-24 on page 8-36.

Figure 8-45 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
```

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

<Configure the remaining transparent interfaces in the slot>
```

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

<Configure the remaining transparent interfaces in the slot>
```

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 8-33 on page 8-50.

Node 1

The configuration for node 1 is the same as described in the “Node 1” section on page 8-58.

Node 2

Figure 8-46 shows the shelf configuration for node 2 in the line card protected meshed ring with unprotected channels shown in Figure 8-33 on page 8-50. Channels 1-4 are line card protected using a west line card motherboard in slot 2 and an east line card motherboard in slot 4. Slot 8 uses an east line card motherboard for the unprotected channels.

Figure 8-46 Shelf Configuration for Node 2 in Line Card Protected Meshed Ring with Unprotected Channels

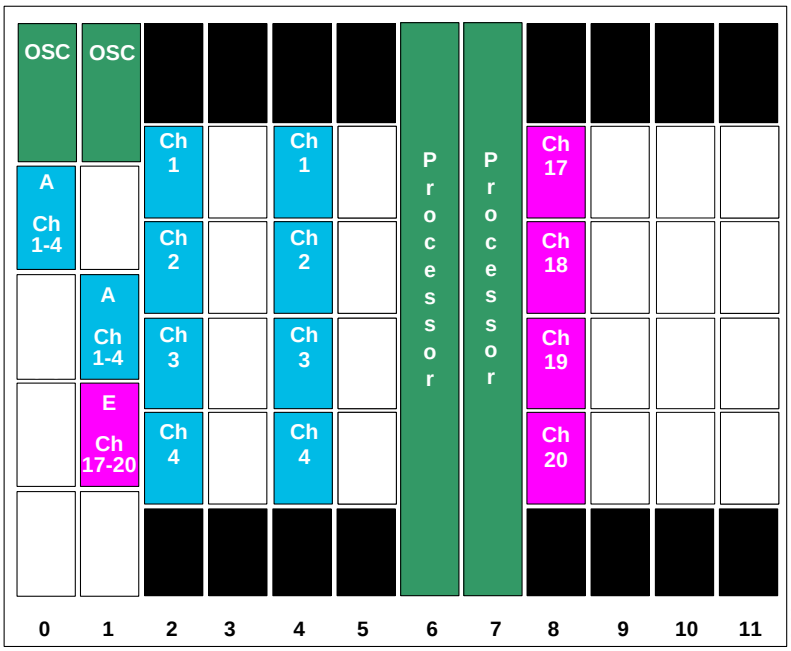
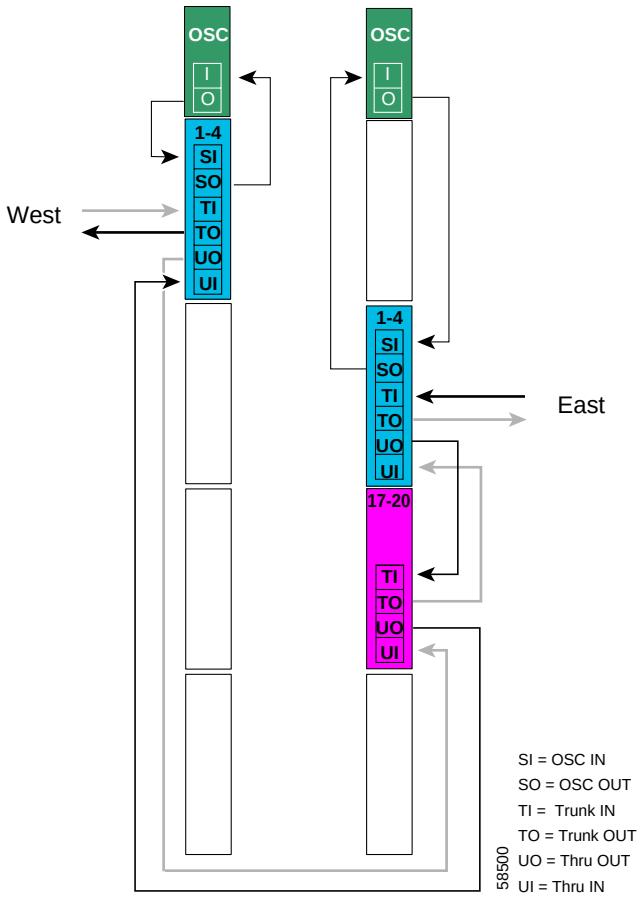


Figure 8-47 shows how the 4-channel mux/demux modules are cabled for node 2 in the line card protected meshed ring with unprotected channels shown in Figure 8-33 on page 8-50.

Figure 8-47 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
```

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

<Configure the remaining transparent interfaces in the slot>
```

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

<Configure the remaining transparent interfaces in the slot>
```

Transparent Interfaces in Slot 8

```
Node2(config)# interface transparent 8/0/0
Node2(config-if)# encapsulation gigabitethernet
Node2(config-if)# monitor enable
Node2(config-if)# exit

<Configure the remaining transparent interfaces in the slot>
```

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 8-48 shows how the modules are installed in the shelf for node 3 in the example network shown in Figure 8-33 on page 8-50. Channels 5–8 are line card protected using an east line card motherboard in slot 3 and a west line card motherboard in slot 5. Channels 13–16 are line card protected using an east line card motherboard in slot 9 and a west line card motherboard in slot 11. Slot 8 uses a west line card motherboard for the unprotected channels.

Figure 8-48 Shelf Configuration for Node 3 in Line Card Protected Meshed Ring with Unprotected Channels

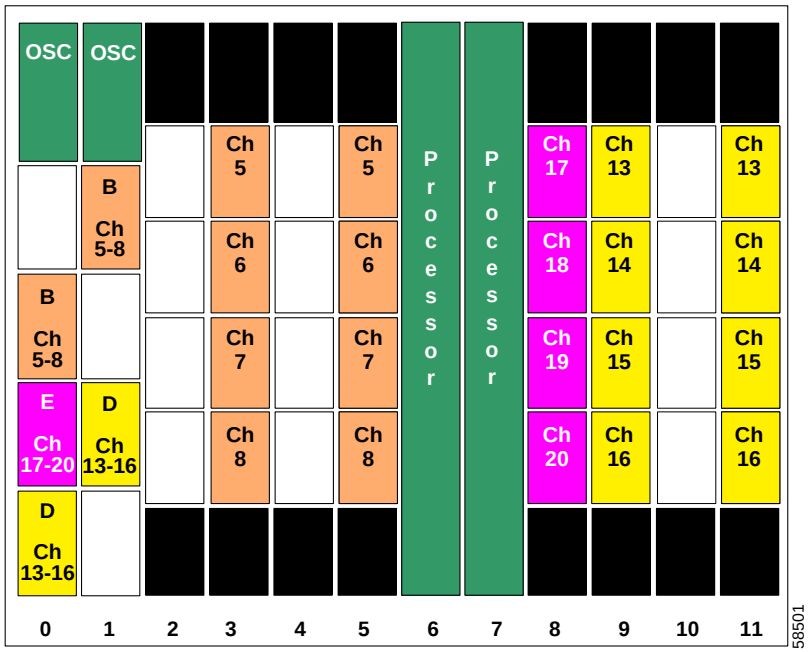
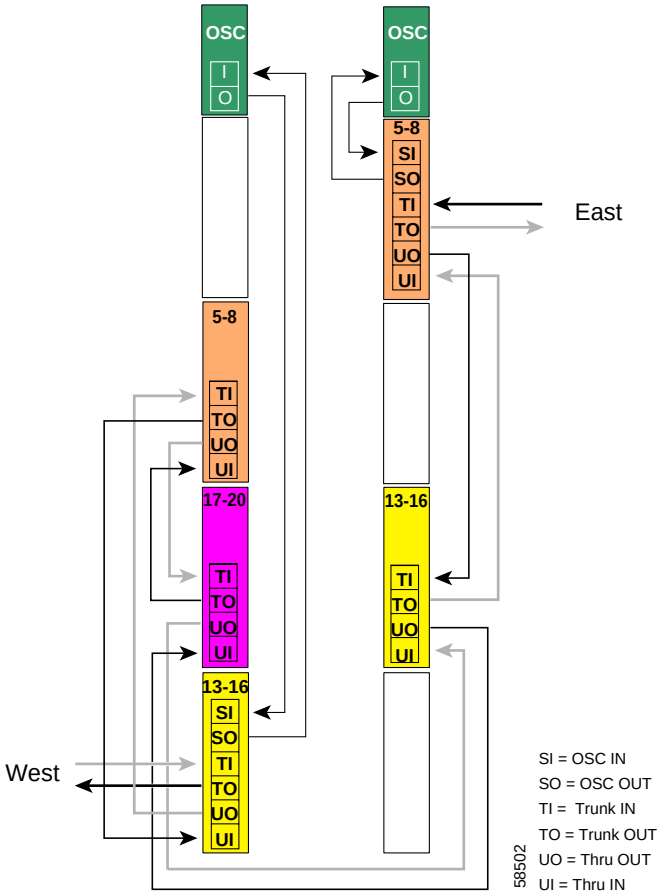


Figure 8-49 shows how the 4-channel mux/demux modules are cabled for node 3 in the line card protected meshed ring with unprotected channels shown in Figure 8-33 on page 8-50.

Figure 8-49 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
```

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

<Configure the remaining transparent interfaces in the slot>
```

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

<Configure the remaining transparent interfaces in the slot>
```

Transparent Interfaces in Slot 8

```
Node3(config)# interface transparent 8/0/0
Node3(config-if)# encapsulation gigabitethernet
Node3(config-if)# monitor enable
Node3(config-if)# exit

<Configure the remaining transparent interfaces in the slot>
```

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

<Configure the remaining transparent interfaces in the slot>
```

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

<Configure the remaining transparent interfaces in the slot>
```

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 8-69.

CHAPTER 9

Monitoring the Network Topology

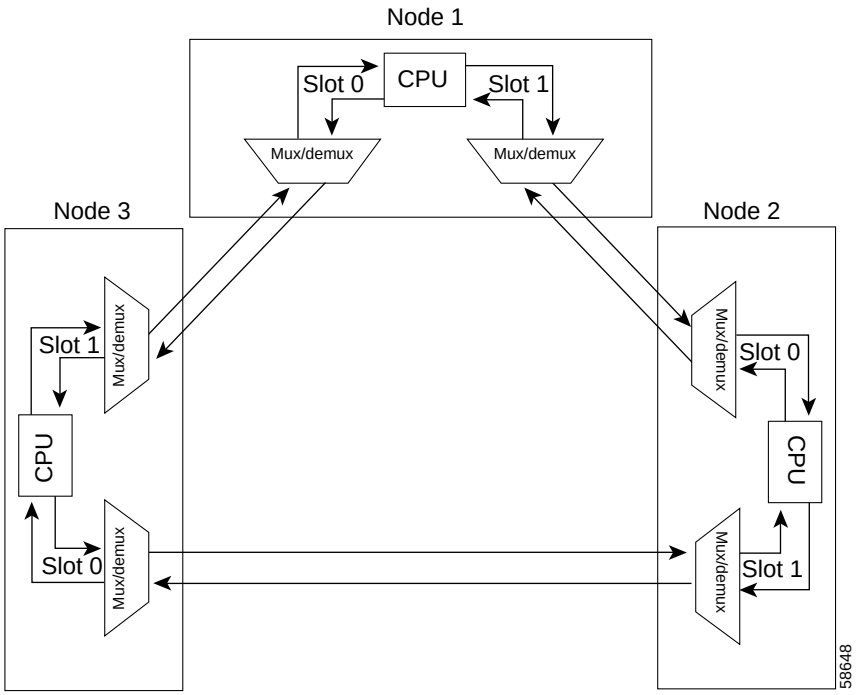
This chapter describes how to configure and manage your network topology. This chapter includes the following sections:

About the OSC

As described in the "Optical Supervisory Channel" section on page 1-8, the Cisco ONS 15540 ESP 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 ESP 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 9-1 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 9-1 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 ESP network with a single Ethernet connection. Also, just one Ethernet connection is required from the NMS to monitor all Cisco ONS 15540 ESP 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 ESP Planning Guide.*

Configuring CDP

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 ESP, 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" section on page 9-15.

Configuring Global CDP

To configure CDP on your Cisco ONS 15540 ESP, 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 *seconds*	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 *seconds*	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 {{***** | *entry-name*} [**protocol** | **version**]}	Displays information about all neighbors or a specific neighbor discovered by CDP. Optionally, displays the protocol and version.
show cdp interface [*type number*]	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

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
clear cdp counters	Resets the CDP traffic counters to zero.
clear cdp table	Clears the table that contains the CDP neighbor information.

Configuring CDP Topology Discovery on Wdm Interfaces

You can enable CDP topology discovery on the wdm interfaces that connect to the trunk fiber. CDP then automatically advertises interface information to neighboring nodes.

Note The Cisco ONS 15540 ESP enables CDP 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** *seconds*	Modifies the interval to hold a nonstatic network topology node entry. The default value is 300 seconds.
Step 2	Switch(config)# **interface wdm** *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 for Wdm Interfaces

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
oscp timer hello interval *milliseconds*	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)# oscp 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
oscp timer hello holddown *milliseconds*	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)# oscp 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
oscp timer inactivity-factor *factor*	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)# oscp 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
show oscp info	Displays the OSCP configuration.

Example

The following example shows the OSCP configuration:

```
Switch(config)# show oscp info
OSCP 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 OSCP 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
show oscp neighbor	Displays the OSCP neighbor status.

Example

The following example shows the OSCP neighbors for a node:

```
Switch(config)# show oscp neighbor
OSCP Neighbors
   Neighbor Node Id:0009.7c1a.cb20   Port list:
    Local Port    Port ID  Rem Port ID OSCP state
   ~~~~~~~~~~~~~ ~~~~~~~~ ~~~~~~~~~~~ ~~~~~~~~~
   Wave0         20E0000   20E0000     2way
```

Configuring IP on the OSC

Configuring IP on the OSC allows you to use one Cisco ONS 15540 ESP node in the network to monitor all the other Cisco ONS 15540 ESP 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 which 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 since 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 unnumber 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** *prefix prefix-mask interface*	Configures IP static routes for some or all destinations.
	or	or
	Switch(config)# **router ospf** *process-id*	Configures OSPF as the routing protocol.
	Switch(config-router)# **network** *network-address wildcard-mask* **area** *area-id*	
	or	or
	Switch(config)# **router eigrp** *as-number*	Configures EIGRP as the routing protocol.
	Switch(config-router)# **network** *network-number* [*network-mask*]	
	or	or
	Switch(config)# **router bgp** *as-number*	Configures BGP as the routing protocol.
	Switch(config-router)# **network** *network-number* [**mask** *network-mask*]	
	Switch(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *number*	

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
telnet *ip-address*	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 SNMP

SNMP is an application-layer protocol that allows an SNMP manager, such an 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 ESP.

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 ESP 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 ESP supports SMNP trap notifications through MIBs. This section describes the following MIBs:

- Alarm threshold MIB
- APS MIB
- Optical monitor 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 ESP 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 *Cisco ONS 15540 ESP MIBs User Quick Reference*.

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
snmp-server enable traps threshold min-severity {**degrade** | **failure**}	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
```

Optical Monitor MIB

The APS MIB (CISCO-OPTICAL-MONITOR-MIB) assists SNMP monitoring of optical monitor activity. To enable the SNMP trap notifications for optical monitor, use the following global configuration command:

Command	Purpose
snmp-server enable traps optical monitor {critical | major | minor | not-alarmed}	Enables SNMP trap notifications for optical monitor 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 critical SNMP trap notifications for optical monitor activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps optical monitor critical
```

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

To take advantage of the OSC, the Cisco ONS 15540 ESP system must be equipped with one mux/demux module with OSC (for unprotected configurations) or two mux/demux modules with OSC (for protected configurations). If your system is not equipped to support the OSC, 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 ESP 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.

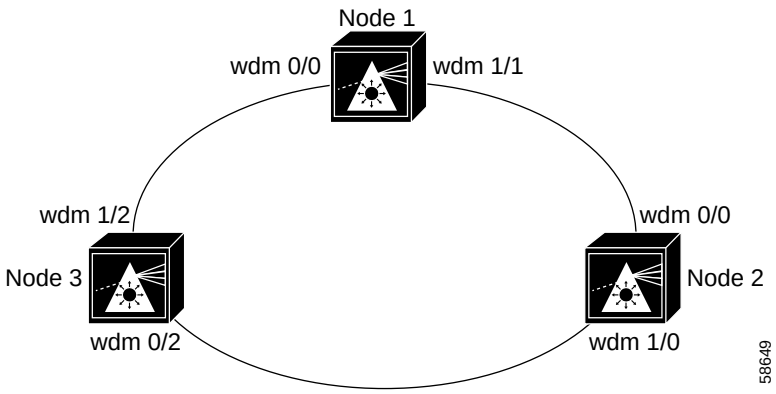
Manually Configuring the Network Topology

If the OSC is absent from the system or CDP is disabled, you must manually add the wdm 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** *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 9-2 shows an example ring topology with three shelves.

Figure 9-2 Ring Topology Example



The following example shows how to configure the network topology for node 1 in Figure 9-2:

```
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 9-2:

```
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 9-2:

```
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
show topology neighbor	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 Transparent Interfaces in the Network Topology

The client-side transparent interfaces on the Cisco ONS 15540 ESP do not support CDP. Therefore, you can explicitly add the transparent interfaces and client equipment to the network topology.

To add a transparent interface to the network topology, perform the following steps on the transparent interfaces on all the nodes in the network, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **interface transparent** *slot*/*subcard*/**0** Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.

	Command	Purpose
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.

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 for Transparent Interfaces

To display the topology information for a transparent interface, use the following EXEC command:

Command	Purpose
show topology neighbor	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 ESP. 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 ESP 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 ESP, perform the following steps:

	Command	Purpose
Step 1	Switch# **dir** {**bootflash:** | **slot***n***:** | **disk***n***:**}	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# **delete** {**bootflash:***filename* | **slot***n***:***filename* | **disk***n***:***filename*}	Deletes an old file to make remove for the new file.
Step 3	Switch# **squeeze** {**bootflash:** | **slot***n***:**}	Recovers the space on the Flash memory device.
Step 4	Switch# **copy tftp:** {**bootflash:** | **slot***n***:** | **disk***n***:**}	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# **delete** {**bootflash:cv/*** | **slot***n***:cv/*** | **disk***n***:cv/***}	Removes existing files from the CiscoView directory.
Step 6	Switch# **squeeze** {**bootflash:** | **slot***n***:** | **disk***n***:**}	Recovers the space in the file system.
Step 7	Switch# **archive tar /xtract bootflash:ONS15540-1.tar bootflash:cv** or Switch# **archive tar /xtract slot***n***:ONS15540-1.tar slot***n***:cv** or Switch# **archive tar /xtract disk***n***:ONS15540-1.tar disk***n***:cv**	Extracts the CiscoView files from the tar file on the TFTP server to the CiscoView directory.
Step 8	Switch# **dir** {**bootflash:** | **slot***n***:** | **disk***n***:**}	Displays the file in Flash memory. Repeat Step 1 and Step 8 for the file system on the standby processor (**sby-bootflash:**, **sby-disk***n***:** or **sby-slot***n***:**).
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.tar
Destination filename [ONS15540.tar]?
Accessing tftp://20.1.1.1/ONS15540.tar...
Loading ONS15540.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.tar slot0:/cv
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC

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.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.tar
Address or name of remote host []? 20.1.1.1
Source filename []? ONS15540.tar
Destination filename [ONS15540.tar]?
Accessing tftp://20.1.1.1/ONS15540.tar...
Loading ONS15540.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.tar sby-slot0:cv
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
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.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 ESP:

```
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.tar
Destination filename [ONS15540.tar]?
Accessing tftp://20.1.1.1/ONS15540.tar...
Loading ONS15540.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.tar slot0:cv
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC

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.tar]?
Destination filename [ONS15540.tar]?
Accessing tftp://20.1.1.1/ONS15540.tar...
Loading ONS15540.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.tar slot0:cv
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
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 ESP 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

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Y