



Cisco ONS 15530 Configuration Guide

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

<http://www.cisco.com>

Tel: 408 526-4000
800 553-NETS (6387)

Fax: 408 526-4100

Customer Order Number: DOC-7816488=
Text Part Number: 78-16488-02



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

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

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

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

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

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0406R)

Cisco ONS 15530 Configuration Guide

Copyright © 2002–2004 Cisco Systems, Inc. All rights reserved.



Preface	xiii
Audience	xiii
New and Changed Information	xiii
New and Changed Information for Cisco IOS Release 12.2(25)S	xiii
New and Changed Information for Cisco IOS Release 12.2(22)S	xiv
Organization	xiv
Related Documentation	xiv
Document Conventions	xv
Obtaining Documentation	xvi
Cisco.com	xvi
Ordering Documentation	xvi
Documentation Feedback	xvii
Obtaining Technical Assistance	xvii
Cisco Technical Support Website	xvii
Submitting a Service Request	xvii
Definitions of Service Request Severity	xviii
Obtaining Additional Publications and Information	xviii

CHAPTER 1

Product Overview	1-1
Cisco ONS 15530 Hardware Features	1-2
Chassis Overview	1-3
Component Summary	1-3
ESCON Aggregation Cards	1-4
8-Port FC/GE Aggregation Cards	1-4
2.5-Gbps ITU Trunk Cards	1-5
10-Gbps ITU Trunk Cards	1-6
10-Gbps Uplink Cards	1-6
Transponder Line Cards	1-6
OADM Modules	1-7
PSMs	1-7
Carrier Motherboards	1-8
OSC Modules	1-8

- VOA Modules 1-8
 - PB-OE Modules 1-8
 - WB-VOA Modules 1-8
- CPU Switch Modules 1-8
 - Switch Fabric 1-9
- Cisco ONS 15530 Software Features 1-9
 - Network Management Systems 1-10
 - Optical Supervisory Channel 1-10
 - In-Band Message Channel 1-11
 - Online Diagnostics 1-11
- Network Topologies 1-11
- Standards Compliance 1-11

CHAPTER 2

Before You Begin 2-1

- About the CLI 2-1
- About Cisco IOS Command Modes 2-1
 - Listing Cisco IOS Commands and Syntax 2-3
- Interface Naming Conventions 2-4
 - ESCON Aggregation Card Interfaces 2-4
 - Esconphy Interfaces 2-5
 - Portgroup Interfaces 2-5
 - 8-Port FC/GE Aggregation Card Interfaces 2-5
 - Gigabitphy Interfaces 2-6
 - Portgroup Interfaces 2-6
 - 2.5-Gbps ITU Trunk Card Interfaces 2-6
 - Ethernetdcc Interfaces 2-7
 - Waveethernetphy Interfaces 2-7
 - Wavepatch Interfaces 2-7
 - 10-Gbps ITU Trunk Card Interfaces 2-8
 - Ethernetdcc Interfaces 2-9
 - Waveethernetphy Interfaces 2-9
 - Waveethernetphy Subinterfaces 2-10
 - Wavepatch Interfaces 2-10
 - 10-Gbps Uplink Card Interfaces 2-10
 - Ethernetdcc Interfaces 2-11
 - Tengigethernetphy Interfaces 2-11
 - Tengigethernetphy Subinterfaces 2-11

Transponder Line Card Interfaces	2-12
Transparent Interfaces	2-12
Wave Interfaces	2-13
Wavepatch Interfaces	2-13
OADM Module Interfaces	2-13
Filter Interfaces	2-14
Oscfilter Interfaces	2-14
Wdm Interfaces	2-14
Thru Interfaces	2-15
PSM Interfaces	2-15
Wdmrelay Interfaces	2-15
Wdmsplit Interfaces	2-15
OSC Card Interfaces	2-16
Wave Interfaces	2-16
CPU Switch Module Interfaces	2-16
NME Interfaces	2-16
Auxiliary Port Interfaces	2-16
WB-VOA Card Interfaces	2-17
Voain Interfaces	2-17
Voayout Interfaces	2-17
PB-OE Module Interfaces	2-18
Voafilterin Interfaces	2-19
Voafilterin Subinterfaces	2-19
Voafilterout Interfaces	2-19
Voabypassout Interfaces	2-20
Voabypassin Interfaces	2-20
Configuration Overview	2-20
CHAPTER 3	Initial Configuration 3-1
	About the CPU Switch Module 3-1
	Starting Up the Cisco ONS 15530 3-2
	Using the Console Ports, NME Ports, and Auxiliary Ports 3-2
	Modem Support 3-3
	About Passwords 3-3
	Enable Password 3-3
	Enable Secret Password 3-3
	Configuring IP Access on the NME Interface 3-4
	Displaying the NME Interface Configuration 3-5
	Displaying the Operating Configurations 3-6

- Configuring the Host Name **3-6**
- About NTP **3-7**
- Configuring NTP **3-7**
 - Displaying the NTP Configuration **3-8**
- Configuring Security Features **3-8**
 - Configuring AAA **3-9**
 - Configuring Authentication **3-9**
 - Configuring Authorization **3-9**
 - Configuring Accounting **3-9**
 - Configuring Kerberos **3-9**
 - Configuring RADIUS **3-10**
 - Configuring TACACS+ **3-10**
 - Configuring Traffic Filters and Firewalls **3-11**
 - Configuring Passwords and Privileges **3-11**
- About CPU Switch Module Redundancy **3-11**
 - Redundant Operation Requirements **3-14**
 - Conditions Causing a Switchover from the Active CPU Switch Module **3-14**
- Configuring CPU Switch Module Redundancy **3-15**
 - Forcing a Switchover from Privileged EXEC Mode **3-15**
 - Forcing a Switchover from ROM Monitor Mode **3-15**
 - Configuring Autoboot **3-17**
 - Displaying the Autoboot Configuration **3-17**
 - Synchronizing the Configurations **3-18**
 - Synchronizing Configurations Manually **3-18**
 - Enabling and Disabling Automatic Synchronization **3-18**
 - Configuring Maintenance Mode **3-19**
 - Displaying the CPU Switch Module Redundancy Configuration and Status **3-20**
 - Reloading the CPU Switch Modules **3-23**
 - Configuring Privileged EXEC Mode Access on the Standby CPU Switch Module **3-23**
 - Displaying the Standby CPU Switch Module Privileged EXEC Mode Status **3-23**
- About the Software Configuration Register **3-24**
 - Software Configuration Register Settings **3-25**
 - Boot Field Values **3-26**
 - Default System Boot Behavior **3-27**
 - Boot Command **3-27**
- Changing the Software Configuration Register **3-28**
 - Verify the Configuration Register Value **3-28**

- About Fan Failure Shutdown 3-29
- Configuring Fan Failure Shutdown 3-29
 - Displaying the Fan Tray Failure Shutdown Configuration 3-30

CHAPTER 4

- Configuring ESCON Aggregation Card Interfaces 4-1**
 - About ESCON Signal Aggregation Support 4-1
 - Configuring ESCON Aggregation Card Interfaces 4-3
 - Displaying the ESCON Aggregation Card Interface Configuration 4-4
 - About Latency and Transmit Buffers 4-5
 - Configuring Transmit Buffer Size 4-6
 - Displaying Transmit Buffer Configuration 4-7
 - About Cross Connections 4-7
 - Configuring Cross Connections 4-8
 - Displaying the Cross Connection Configuration 4-9
 - About Alarm Thresholds 4-9
 - Configuring Alarm Thresholds 4-9
 - Displaying the Alarm Threshold Configuration 4-11

CHAPTER 5

- Configuring 8-Port FC/GE Aggregation Card Interfaces 5-1**
 - About the 8-Port FC/GE Aggregation Card 5-1
 - Protocol Monitoring 5-2
 - Support for FC Port Types 5-3
 - Configuring 8-Port FC/GE Aggregation Card Interfaces 5-3
 - Displaying the 8-Port FC/GE Aggregation Card Interface Configuration 5-5
 - About Latency and Transmit Buffers 5-6
 - Configuring Transmit Buffer Size for FC and FICON 5-7
 - Displaying Transmit Buffer Configuration 5-8
 - About Cross Connections 5-9
 - Configuring Cross Connections 5-10
 - Displaying the Cross Connection Configuration 5-10
 - About Alarm Thresholds 5-11
 - Configuring Alarm Thresholds 5-11
 - Displaying the Alarm Threshold Configuration 5-12

CHAPTER 6

- Configuring Transponder Line Card Interfaces 6-1**
 - Configuring Protocol Encapsulation or Clock Rate 6-2
 - Displaying Protocol Encapsulation or Clock Rate Configuration 6-5

- About Transponder Line Card Channel Frequencies 6-6
- Configuring Transponder Line Card Channel Frequency 6-6
 - Displaying Transponder Line Card Channel Frequency 6-6
- About Protocol Monitoring 6-7
- Configuring Protocol Monitoring 6-9
 - Displaying Protocol Monitoring Configuration 6-9
- About Alarm Thresholds 6-10
- Configuring Alarm Thresholds 6-11
 - Displaying Alarm Threshold Configuration 6-13
- About Laser Shutdown 6-14
 - About Forward Laser Control 6-14
 - About OFC 6-15
 - About Laser Safety Control 6-16
- Configuring Laser Shutdown 6-17
 - Configuring Forward Laser Control 6-17
 - Displaying Forward Laser Control Configuration 6-18
 - Configuring Laser Safety Control 6-18
 - Displaying Laser Safety Control Configuration 6-19
- Configuring Optical Power Thresholds 6-19
 - Displaying Optical Power Threshold Configuration 6-20
- About Patch Connections 6-21
- Configuring Patch Connections 6-21
 - Displaying Patch Connections 6-22
- About Cross Connections 6-23
 - Displaying Cross Connections 6-23

CHAPTER 7

- Configuring Trunk and Uplink Card Interfaces 7-1**
 - Configuring 2.5-Gbps ITU Trunk Card Interfaces 7-1
 - Displaying the 2.5-Gbps ITU Trunk Card Interface Configuration 7-3
 - Configuring 10-Gbps ITU Trunk Card Interfaces 7-4
 - Displaying the 10-Gbps ITU Trunk Card Interface Configuration 7-5
 - Configuring 10-Gbps Uplink Card Interfaces 7-7
 - Displaying the 10-Gbps Uplink Card Interface Configuration 7-8
- About Cross Connections 7-9
- Configuring Cross Connections 7-10
 - Displaying the Cross Connection Configuration 7-11

About Alarm Thresholds	7-11
Configuring Alarm Thresholds	7-12
Displaying the Alarm Threshold Configuration	7-13
About Patch Connections	7-15
Configuring Patch Connections	7-15

CHAPTER 8

Configuring VOA Module Interfaces	8-1
About Variable Optical Attenuation	8-1
VOA Modules	8-2
Single WB-VOA Modules	8-2
Dual WB-VOA Modules	8-3
Single Band PB-OE Modules	8-3
Dual Band PB-OE	8-4
Configuring VOA Module Interfaces	8-5
Configuring Attenuation	8-5
Configuring Automatic Attenuation	8-6
Configuring Manual Attenuation	8-6
Displaying the Attenuation Configuration	8-7
About Optical Thresholds	8-8
Configuring Optical Receive Power Thresholds	8-8
Displaying the Optical Threshold Configuration	8-9

CHAPTER 9

Configuring PSM Interfaces	9-1
Enabling Wdmsplit Interfaces	9-1
Displaying Wdmsplit Interface Information	9-2
Configuring Trunk Fiber Based Protection	9-2
Displaying Trunk Fiber Protection Configuration	9-3
About Switchovers and Optical Power Thresholds	9-3
Unamplified Topologies	9-4
Post-Amplified Topologies	9-5
Post-Amplified and Preamplified Topologies	9-6
Configuring Optical Power Thresholds	9-7
Displaying Optical Power Threshold Configuration	9-8
Configuring Patch Connections	9-9
Displaying Patch Connections	9-9
Configuring Wdmsplit Interfaces in the Network Topology	9-10
Displaying Topology Information for Wdmsplit Interfaces	9-11

CHAPTER 10

Configuring APS 10-1

- About APS **10-2**
- About Splitter Protection **10-2**
 - Considerations for Using Splitter Protection **10-4**
- Configuring Splitter Protection **10-5**
 - Displaying the Splitter Protection Configuration **10-6**
- About Line Card Protection **10-7**
- About Client Based Line Card Protection **10-7**
- About Y-Cable Line Card Protection **10-9**
 - Considerations for Using Y-Cable Based Line Card Protection **10-10**
- Configuring Y-Cable Based Line Card Protection **10-11**
 - Displaying the Y-Cable Protection Configuration **10-12**
- About Switch Fabric Based Line Card Protection **10-13**
 - Considerations for Using Switch Fabric Based Line Card Protection **10-14**
- Configuring Switch Fabric Based Line Card Protection **10-14**
 - Displaying Switch Fabric Based Protection Configuration **10-15**
- About Trunk Fiber Based Protection **10-16**
 - Considerations for Using Trunk Fiber Protection **10-17**
- Configuring Trunk Fiber Protection **10-17**
 - Displaying Trunk Fiber Protection Configuration **10-18**
- About Redundant Switch Fabric Protection **10-18**
- Configuring APS Group Attributes **10-19**
 - Configuring Revertive Switching **10-19**
 - Displaying the Revertive Switching Configuration **10-20**
 - About Unidirectional and Bidirectional Path Switching **10-21**
 - About APS Switching for Cisco ONS 15216 OADMs **10-23**
 - Configuring Unidirectional and Bidirectional Path Switching **10-23**
 - Displaying the Unidirectional and Bidirectional Path Switching Configuration **10-27**
 - Configuring the Switchover-Enable Timer **10-27**
 - Displaying the Switchover-Enable Timer Configuration **10-28**
- About Switchovers and Lockouts **10-29**
- Requesting a Switchover or Lockout **10-30**
 - Displaying Switchover and Lockout Request Status **10-30**
- Clearing Switchovers and Lockouts **10-31**
 - Displaying Switchover and Lockout Clear Status **10-31**

CHAPTER 11**Configuring Multiple Shelf Nodes 11-1**

- About Multiple Shelf Nodes 11-1
- Configuring Multiple Shelf Nodes 11-1
 - Configuring Patch Connections Between Shelves 11-2
 - Configuring APS 11-3

CHAPTER 12**Monitoring Your Network Topology 12-1**

- About the OSC 12-1
 - Hardware Guidelines for Using OSC 12-2
- Configuring CDP 12-3
 - Configuring Global CDP 12-3
 - Displaying the Global CDP Configuration 12-3
 - Displaying Global CDP Information 12-4
 - Clearing Global CDP Information 12-5
 - Configuring CDP Topology Discovery on Wdm Interfaces 12-5
 - Displaying CDP Information for Wdm Interfaces 12-6
- Configuring OSCP 12-6
 - Configuring the Hello Interval Timer 12-6
 - Configuring the Hello Hold-Down Timer 12-7
 - Configuring the Inactivity Factor 12-7
 - Displaying the OSCP Configuration 12-8
 - Displaying OSCP Neighbors 12-8
- Configuring IP on the OSC 12-8
 - Displaying the OSC Configuration 12-11
 - Verifying Connectivity on the OSC 12-12
- Configuring IP on Ethernetdcc Interfaces for the In-Band Message Channel 12-12
 - Displaying the Ethernetdcc Interface Configuration 12-14
 - Verifying Connectivity over the In-Band Message Channel 12-14
- Configuring SNMP 12-15
 - Enabling MIB Notifications 12-15
 - Alarm Threshold MIB 12-15
 - APS MIB 12-16
 - CDL MIB 12-16
 - Optical Monitor MIB 12-17
 - OSCP MIB 12-17
 - Patch MIB 12-17
 - Physical Topology MIB 12-18
 - Redundancy Facility MIB 12-18

- Monitoring Without the OSC or In-Band Message Channel 12-19
 - Setting up Connections to Individual Nodes 12-19
 - Manually Configuring the Network Topology 12-19
 - Displaying the Network Topology 12-20
- Configuring Interfaces in the Network Topology 12-21
 - Displaying Topology Information 12-22
- About Embedded CiscoView 12-22
- Installing and Configuring Embedded CiscoView 12-22
 - Accessing Embedded CiscoView 12-25
 - Displaying Embedded CiscoView Information 12-25

INDEX



Preface

This preface describes the audience, organization, and conventions for the *Cisco ONS 15530 Configuration Guide*, and provides information on how to obtain related documentation.

The information contained in this document pertains to the entire range of hardware components and software features supported on the Cisco ONS 15530 platform. As new hardware and Cisco IOS software releases are made available for the Cisco ONS 15530 platform, verification of compatibility becomes extremely important. To ensure that your hardware is supported by your release of Cisco IOS software, see the [“New and Changed Information” section on page xiii](#). Also refer to the “Hardware Supported” section of the latest release notes the Cisco ONS 15530.

Audience

This publication is intended for experienced network administrators who are responsible for configuring and maintaining the Cisco ONS 15530.

New and Changed Information

This section describes the changes and additions to this guide for the releases of the Cisco IOS Release 12.2S major release for the Cisco ONS 15530.

New and Changed Information for Cisco IOS Release 12.2(25)S

The following table lists the changes and additions to this guide for Cisco IOS Release 12.2(25)S

Feature	Description	Location
ISC links peer mode 1-Gbps support on transponder modules.	The transponders modules support ISC links peer mode at 1 Gbps as well as 2 Gbps.	“Transponder Line Cards” section on page 1-6 “Configuring Protocol Encapsulation or Clock Rate” section on page 4-2 “About Protocol Monitoring” section on page 6-7

New and Changed Information for Cisco IOS Release 12.2(22)S

The following table lists the changes and addition to this guide for Cisco IOS Release 12.2(22)S.

Feature	Description	Location
Monitoring for 2-Gbps protocols	The 2.5-Gbps transponder module now supports monitoring for 2-Gbps FC and FICON.	

Organization

This guide is organized as follows:

Chapter	Title	Description
Chapter 1	Product Overview	Provides an overview of the Cisco ONS 15530 features and functions.
Chapter 2	Before You Begin	Describes basic information about the Cisco ONS 15530 CLI interface, IOS mode and naming conventions.
Chapter 3	Initial Configuration	Describes the initial configuration of the Cisco ONS 15530.
Chapter 4	Configuring ESCON Aggregation Card Interfaces	Describes how to configure ESCON interfaces.
Chapter 5	Configuring 8-Port FC/GE Aggregation Card Interfaces	Describes how to configure 8-port FC/GE aggregation card interfaces.
Chapter 6	Configuring Transponder Line Card Interfaces	Describes how to configure transponder interfaces and patch connections.
Chapter 7	Configuring Trunk and Uplink Card Interfaces	Describes how to configure the trunk cards.
Chapter 8	Configuring VOA Module Interfaces	Describes how to configure PB-OE modules and WB-VOA modules for signal attenuation.
Chapter 9	Configuring PSM Interfaces	Describes how to configure protection switch module interfaces for trunk fiber protection.
Chapter 10	Configuring APS	Describes how to configure signal protection on Cisco ONS 15530 systems and networks.
Chapter 11	Configuring Multiple Shelf Nodes	Describes how to configure a network node with multiple Cisco ONS 15530 shelves supporting more than four channels with line card protection.
Chapter 12	Monitoring Your Network Topology	Describes how to monitor the operation of Cisco ONS 15530 networks.

Related Documentation

This document provides detailed configuration examples for the Cisco ONS 15530; however, it does not provide complete extensive background information on DWDM (dense wavelength division multiplexing) technology or the architecture of the Cisco ONS 15530. For background information on DWDM technology, refer to the [Introduction to DWDM Technology](#) document.

You will also find useful information on the CLI (command-line interface) and basic shelf management in the [Cisco IOS Configuration Fundamentals Configuration Guide](#) and the [Cisco IOS Configuration Fundamentals Command Reference](#) publication.

Refer to the following documents for detailed design considerations, hardware installation, safety information, troubleshooting information, and glossary terms:

- [Regulatory Compliance and Safety Information for the Cisco ONS 15500 Series](#)
- [Cisco ONS 15530 Planning Guide](#)
- [Cisco ONS 15530 Hardware Installation Guide](#)
- [Cisco ONS 15530 Optical Transport Turn-Up and Test Guide](#)
- [Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections](#)
- [Cisco ONS 15530 Command Reference](#)
- [Cisco ONS 15530 TL1 Command Command Reference](#)
- [Cisco ONS 15530 System Alarms and Error Messages](#)
- [Cisco ONS 15530 Troubleshooting Guide](#)
- [Network Management for the Cisco ONS 15530](#)
- [MIB Quick Reference for the Cisco ONS 15500 Series](#)
- [Cisco ONS 15530 Software Upgrade Guide](#)

Document Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in boldface .
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> .
[]	Elements in square brackets are optional.
{ x y z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in screen font.

Convention	Description
boldface screen font	Information you must enter is in boldface screen font .
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .
→	This pointer highlights an important line of text in an example.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.

Notes use the following conventions:



Note

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

Cautions use the following conventions:



Caution

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

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/univercd/home/home.htm>

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

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

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

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year at this URL:

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

Access to all tools on the Cisco Technical Support 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>

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 automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC 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 TAC 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)—Your 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 operation 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 your network is impaired, but 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.

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

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

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:
<http://cisco.com/univercd/cc/td/doc/pcat/>
- *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>
- *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>
- 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 15530 is a highly modular and scalable optical switching and aggregation platform. With the Cisco ONS 15530, 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 15530 Planning Guide](#).

The Cisco ONS 15530 is designed to meet and exceed the most stringent ISP (Internet service provider) requirements for product availability and reliability. Its features include:

- Redundant fan assemblies
- Redundant power (AC or DC)
- Redundant CPU switch modules
- Interfaces that can be configured for redundancy using SONET 1+1 APS (Automatic Protection Switching)
- Line cards, power supplies, and fan assemblies that are hot-swappable without powering down the shelf

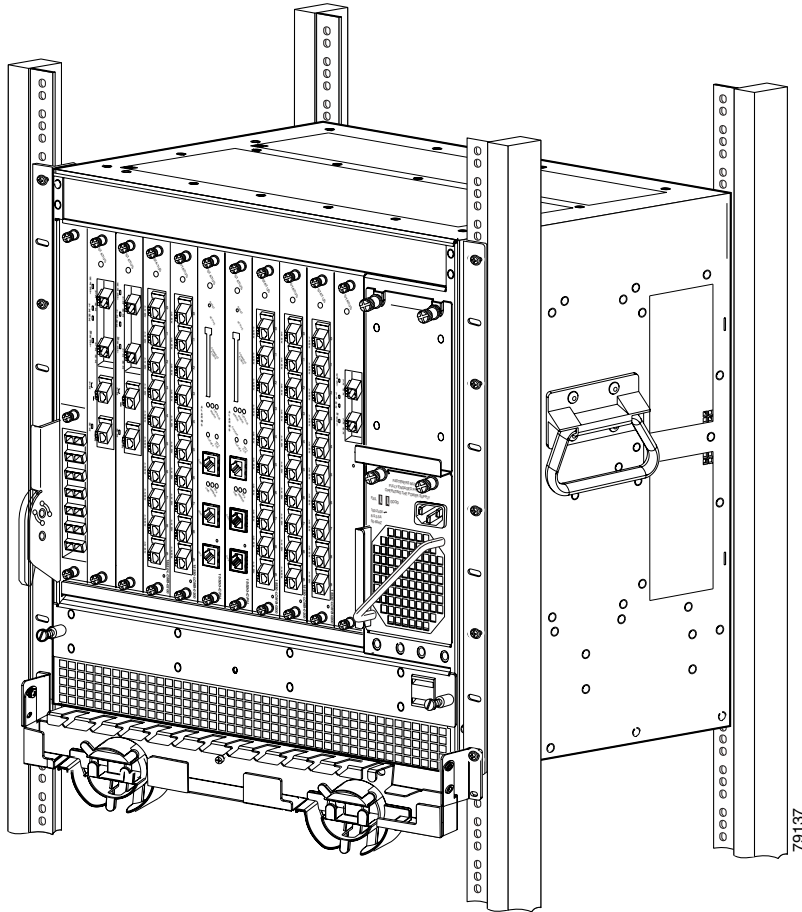
This chapter includes the following sections:

- [Cisco ONS 15530 Hardware Features, page 1-2](#)
- [Cisco ONS 15530 Software Features, page 1-9](#)
- [Network Topologies, page 1-11](#)
- [Standards Compliance, page 1-11](#)

Cisco ONS 15530 Hardware Features

This section describes the hardware features and components of the Cisco ONS 15530. See [Figure 1-1](#).

Figure 1-1 Cisco ONS 15530 Shelf



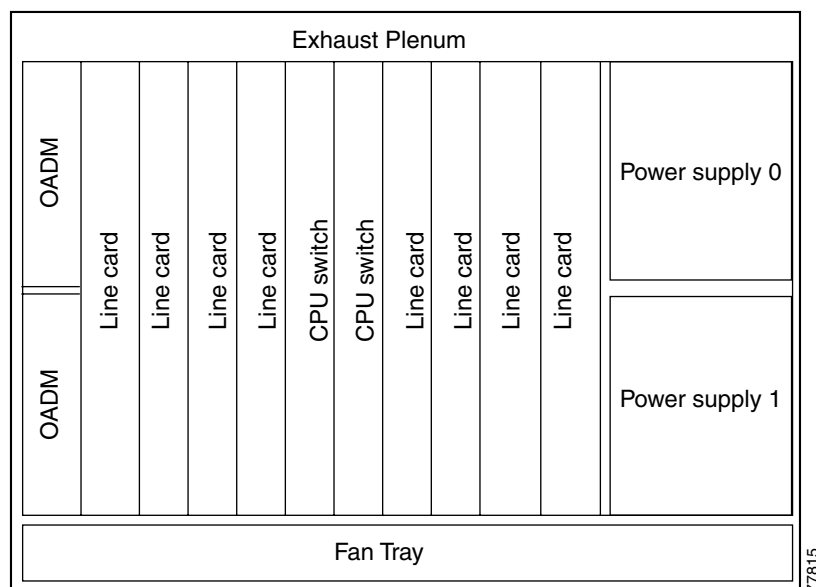
Chassis Overview

The Cisco ONS 15530 is available in two configurations, NEBS and ETSI. Both have two vertically stacked half-height slots specifically for the OADM (optical add/drop multiplexers) modules, and 10 vertically oriented slots that hold the CPU switch modules, line cards, and transponder line cards. As you face the chassis, the leftmost slot (slot 0) holds two half height OADM modules. Slots 1 through 4 and slots 7 through 10 hold the line cards and transponder line cards. Slots 5 and 6 hold the CPU switch modules (see [Figure 1-2](#)). Power supplies are located on the right side of the chassis next to slot 10. Air inlet and fan tray are located beneath the slots. Cable management is located above and beneath the slots. The system has an electrical backplane for system control. All optical connections are located on the front of the shelf.

The Cisco ONS 15530 supports up to 60 ESCON (Enterprise Systems Connectivity) ports on a single shelf and up to 160 ESCON ports in a stacked shelf solution.

[Figure 1-2](#) shows the shelf slot layout.

Figure 1-2 Cisco ONS 15530 Shelf Layout



Component Summary

The Cisco ONS 15530 supports the following hot-swappable modular hardware components:

- 10-port ESCON aggregation cards
- 2.5-Gbps ITU trunk cards
- 10-Gbps ITU trunk cards
- 10-Gbps uplink cards
- 8-port Fibre Channel/Gigabit Ethernet aggregation card
- Single-mode and multimode transponder line cards
- OADM (optical add/drop multiplexer) modules
- PSMs (protection switch modules)

- Carrier motherboards
- OSC (optical supervisory channel) modules
- PB-OE (per-band optical equalizer) modules
- WB-VOA (wide-band variable optical attenuator) modules
- CPU switch modules

ESCON Aggregation Cards

The ESCON aggregation card aggregates up to 10 client data streams into a single 2.5-Gbps signal. The card sends a signal through the switch fabric to a 2.5-Gbps ITU trunk card, 10-Gbps ITU trunk card, or a 10-Gbps uplink card.

[Table 1-1](#) lists features for the SFP optics supported by the ESCON aggregation cards.

Table 1-1 ESCON Aggregation Card SFP Optics Features

Part Number	Description	Fiber Type	Wavelength	Connector Type
15500-XVRA-01A2	Fixed rate	MM 50/125 μm MM 62.5/125 μm	1310 nm	MT-RJ
15500-XVRA-10A1	Low-band variable rate 16 Mbps to 200 Mbps	MM 50/125 μm MM 62.5/125 μm	1310 nm	LC
15500-XVRA-10B1	Low-band variable rate 16 Mbps to 200 Mbps	SM 9/125 μm	1310 nm	LC



Note

The Cisco IOS software only supports Cisco-certified SFP optics on the ESCON aggregation card.

For more information on power budget planning, refer to the [Cisco ONS 15530 Planning Guide](#). For power budget specifications for individual components, refer to the [Cisco ONS 15530 Hardware Installation Guide](#).

8-Port FC/GE Aggregation Cards

The 8-port FC/GE aggregation card aggregates up to eight FC, FICON, GE, or ISC-3 (InterSystem Channel) links compatibility mode data streams into up to four 2.5-Gbps signals. The cards send a signal through the switch fabric to a 2.5-Gbps ITU trunk card, a 10-Gbps ITU trunk card, or a 10-Gbps uplink card.

[Table 1-2](#) lists features for the SFP optics supported by the 8-port FC/GE aggregation cards.

Table 1-2 8-Port FC/GE Aggregation Card SFP Optics Features

Part Number	Protocols or Clock Rate Range Supported	Fiber Type	Wavelength	Connector Type
15500-XVRA-02C1	Gigabit Ethernet ¹ , Fibre Channel (1 Gbps) ² , FICON (1 Gbps), ISC-3 links compatibility mode (1 Gbps)	MM 50/125 μm MM 62.5/125 μm	850 nm	LC
15500-XVRA-03B1	Gigabit Ethernet ³ , Fibre Channel (1 Gbps) ⁴ , FICON (1 Gbps), ISC-3 links compatibility mode (1 Gbps)	SM 9/125 μm	1310 nm	LC
15500-XVRA-11B1	Mid-band variable rate 200 Mbps to 1.25 Gbps	SM	1310 nm	LC
15500-XVRA-12B1	High-band variable rate 1.062 Gbps to 2.488 Gbps	SM	1310 nm	LC

1. 1000BASE-SX
2. FC-0-100-M5-SN-S and FC-0-100-M6-SN-S standards
3. 1000BASE-LX
4. FC-0-100-SM-LC-S standard

**Note**

The Cisco IOS software only supports Cisco-certified SFP optics on the 8-port FC/GE aggregation card.

For more information on power budget planning, refer to the [Cisco ONS 15530 Planning Guide](#). For power budget specifications for individual components, refer to the [Cisco ONS 15530 Hardware Installation Guide](#).

2.5-Gbps ITU Trunk Cards

The 2.5-Gbps ITU trunk card converts an aggregated 2.5-Gbps signal to an ITU-compliant wavelength, or channel. The Cisco ONS 15530 supports two types of 2.5-Gbps ITU trunk cards:

- Splitter—Sends the channels to two OADM modules.
- Nonsplitter—Sends the channel to only one OADM module.

The 2.5-Gbps ITU trunk card has a transmit (laser) power in the range of 5 to 10 dBm and a receive detector sensitivity range of -8 to -28 dBm.

For more information on power budget planning, refer to the [Cisco ONS 15530 Planning Guide](#). For power budget specifications for individual components, refer to the [Cisco ONS 15530 Hardware Installation Guide](#).

10-Gbps ITU Trunk Cards

The 10-Gbps ITU trunk card converts up to four aggregated signals to an ITU-compliant wavelength, or channel. The Cisco ONS 15530 supports two types of two types of 10-Gbps ITU trunk cards:

- Splitter—Sends the channels to two OADM modules.
- Nonsplitter—Sends the channel to only one OADM module.

The 10-Gbps ITU trunk card has an transmit (laser) power in the range of 1 to 5 dBm and a receive detector sensitivity range of -22 to -8 dBm.

For more information on power budget planning, refer to the [Cisco ONS 15530 Planning Guide](#). For power budget specifications for individual components, refer to the [Cisco ONS 15530 Hardware Installation Guide](#).

10-Gbps Uplink Cards

The 10-Gbps uplink card converts up to four aggregated signals to a 10 Gbps 1310-nm signal that can be transmitted to another shelf, such as the Cisco ONS 15540 ESPx and the Cisco ONS 15540. The transmit power for the 10-Gbps uplink card is -8.2 to 0.5 dBm and the receive detector range is -14.4 to 0.5 dBm.

For more information on power budget planning, refer to the [Cisco ONS 15530 Planning Guide](#). For power budget specifications for individual components, refer to the [Cisco ONS 15530 Hardware Installation Guide](#).

Transponder Line Cards

The protocol-transparent and bit-rate transparent transponder line card converts a single client signal into an ITU wavelength, or channel. The Cisco ONS 15530 shelf holds up to four transponder line cards, one for each wavelength supported by the OADM modules.

The Cisco ONS 15530 supports four types of single client interface transponder line cards:

- SM (single-mode) nonsplitter
- SM splitter
- MM (multimode) nonsplitter
- MM splitter

Both types of SM transponder line cards 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. Both types of MM transponder line cards accept SM and MM client signals on the 1310-nm wavelength through an SC connector and support client signal clock rates ranging from 16 Mbps to 622 Mbps.

The transponder line cards are hot pluggable, permitting in-service upgrades and replacement.

All client signals on the transponders are supported in 3R (reshape, retime, retransmit) mode, regardless of protocol encapsulation type. The following protocol encapsulation types are supported in 3R mode plus protocol monitoring:

- ESCON (200 Mbps) SM and MM
- Fibre Channel (1 Gbps and 2 Gbps) SM
- FICON (Fiber Connection) (1 Gbps and 2 Gbps) SM

- Gigabit Ethernet (1250 Mbps) SM
- ISC (InterSystem Channel) links compatibility mode SM
- ISC links peer mode (1-Gbps and 2-Gbps) SM
- SDH (Synchronous Digital Hierarchy) STM-1 SM and MM
- SDH STM-4 SM and MM
- SDH STM-16 SM
- SONET OC-3 SM and MM
- SONET OC-12 SM and MM
- SONET OC-48 SM

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

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

The client interfaces also support the OFC (open fiber control) safety protocol for Fibre Channel, ISC compatibility mode, and FICON. Client-side interfaces are protocol transparent and can accept signals at specific rates between 16 Mbps and 2.5 Gbps.

On the trunk side, the transponder line card has an output (laser) power in the range of 5 to 10 dBm and a receive detector sensitivity range of -22 to -8 dBm. For more information on power budget planning, refer to the [Cisco ONS 15530 Planning Guide](#). For power budget specifications for individual components, refer to the [Cisco ONS 15530 Hardware Installation Guide](#).

OADM Modules

The Cisco ONS 15530 supports one OADM module in an unprotected configuration or two OADM modules for a protected configuration. Each OADM module can multiplex and demultiplex a band of 4 channels. Channels not filtered by the OADM module are passed on to the next OADM module. In a protected configuration, both OADM modules support the same band of channels to provide fault tolerance.

PSMs

The PSM (protection switch module) provides trunk fiber protection for Cisco ONS 15530 systems configured in point-to-point topologies. The PSM sends the signal from an OADM module, ITU trunk card, or transponder line card to both the west and east directions. It receives both the west and east signals and selects one to send to the OADM module, ITU trunk card, or transponder line card. If a trunk fiber cut occurs on the active path, the PSM switches the received signal to the standby path. Because the PSM occupies one of the OADM subslots in the shelf, it protects a maximum of four channels.

The PSM also has an optical monitor port for testing the west and east receive signals. This port samples one percent of these signals, which can be monitored with an optical power meter.

Carrier Motherboards

The carrier motherboard installs into a single shelf slot and accepts two half-size modules. The carrier motherboard supports the OSC modules and the VOA modules.

OSC Modules

The OSC cards support 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 requiring a separate Ethernet connection to each node in the network. Up to two OSC modules can be installed in the carrier motherboard, one card for the west direction and one for the east direction.

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 OADM modules are treated as either express (pass-through) or add/drop channels.

VOA Modules

The Cisco ONS 15530 supports VOA (variable optical attenuator) modules that work with EDFAs (erbium-doped fibre attenuators) to expand DWDM optical networks over greater distances. The VOA modules include PB-OE (per-band optical equalizer) modules and WB-VOA (wide-band variable optical attenuator) modules. These modules are installed in the carrier motherboard.

PB-OE Modules

The PB-OE modules select and attenuate one or two specific 4-channel bands. The Cisco ONS 15530 supports eight single band PBOE modules for bands A through H and four dual band PB-OE modules for bands AB, CD, EF, and GH.

WB-VOA Modules

The WB-VOA modules accept and attenuate an ITU signal regardless of the channels in the signal. This includes signals with a single channel, a band of channels, or multiple bands of channels. There are two types of WB-VOA modules: single and dual. The single WB-VOA module attenuates only one signal and the dual WB-VOA module attenuates up to two signals.

CPU Switch Modules

The Cisco ONS 15530 includes one CPU switch module with a switch fabric. There may be two CPU switch modules in a Cisco ONS 15530 shelf to provide a higher level of system availability. One of the CPU switch modules is the active one (sometimes called primary or master) and the other is the standby (sometimes called secondary, backup, or slave). The standby CPU switch module is present for increased reliability so that it can take over in case the active CPU switch module fails.

Each CPU switch module has a number of subsystems, including a processor, a switch fabric, a clock subsystem, an Ethernet switch for communication between processors and with the LRC (line card redundancy controller) on the OADM modules and line cards, and an SRC (switchcard redundancy

controller). The active processor controls the system. All LRCs in the system use the system clock and synchronization signals from the active CPU switch module. Interfaces on the CPU switch modules permit access by 10/100 Ethernet, console terminal, or modem connections.

The key features of the Cisco ONS 15530 CPU switch module are:

- 32 by 32 port non-blocking crosspoint switch fabric with up to 3.125 Gbps per port
- RM7000 64-bit RISC processor with internal cache
- Galileo GT96100 support chip
- Flash SIMM in a socket for up to 32 MB with a default of 16 MB
- Bootflash PROM for up to 512KB
- NVRAM for up to 512KB with time of day clock
- Console and auxiliary serial port with RS-232C interface
- 10/100 MB NME (network management Ethernet) port
- CompactFlash card slot
- System clocking source
- Support for two CPU switch modules
- Operates from 12 V DC from the backplane with on-card generation of 5, 3.3, 2.5 and 1.8 V DC
- Environmental and system monitoring and control
- 9-port Fast Ethernet Switch for communication to line cards
- SRC (switch redundancy controller) for communicating with line cards

Switch Fabric

The switch fabric, which is integrated onto the CPU switch module, is a 36 by 37 crosspoint, nonblocking switch with only 32 by 32 ports used. Each port carries 3.125 Gbps.

The switch fabric has a built-in protection switch that offers less than 10 ms switching time as a standard feature. This allows uniform performance over a wide wavelength range. The built-in optical power output measurement system has a wide dynamic range of -20 dBm to 20 dBm. In addition it offers fast connection setups coupled with lower level adjustment to enable fast network configuration changes.

Cisco ONS 15530 Software Features

The Cisco ONS 15530 offers the following software functionality:

- Cisco IOS software on the CPU switch module.
- Autoconfiguration at system boot.
- Autodiscovery of network neighbors.
- Power-on diagnostics.
- Online diagnostics.
- CPU switch module 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 CPU switch modules.

- Support for in-service software upgrades.
- Support for per-channel APS (Automatic Protection Switching) in point-to-point, ring, and mesh topologies using redundant subsystems that monitor link integrity and signal quality.
- Trunk fiber based DWDM signal protection using APS in point-to-point topologies.
- Unidirectional and bidirectional 1+1 path switching.
- System configuration and management through the CLI (command-line interface), accessible through an Ethernet connection or the console terminal.
- Optical power monitoring on the signal from the trunk, digital monitoring on both client and trunk interfaces, and per-channel in-service and out-of-service loopback (client and trunk sides).
- Optional out-of-band management of other Cisco ONS 15530 systems on the network through the OSC (optical supervisory channel).
- In-band management of other Cisco ONS 15530 systems using the in-band message 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 15530 is supported by the following network management systems:

- CiscoView
- CTM (Cisco Transport Manager)

For Embedded CiscoView configuration information, see the [“Installing and Configuring Embedded CiscoView” section on page 12-22](#).

For more information on the network management systems that support the Cisco ONS 15530, refer to the [Network Management for the Cisco ONS 15530](#) document.

Optical Supervisory Channel

The Cisco ONS 15530 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 15530 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 OADM 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 15530 systems can be managed individually by separate Ethernet connections.

The OSC is supported by separate modules and motherboards. 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 15530 networks, see [Chapter 12, “Monitoring Your Network Topology.”](#)

In-Band Message Channel

The in-band message channel establishes a method for providing OAM&P (operations, administration, management, and provisioning) functions in Ethernet packet-based optical networks without a SONET layer or SDH layer. In addition, the in-band message channel enables statistical multiplexing of multiple logical lower-speed signals, such as ESCON signals, within a single optical data channel. The in-band message channel terminates with the data channel, not at each node as does the OSC, thus providing management on a per wavelength basis.

Online Diagnostics

The Cisco ONS 15530 provides the following types of online diagnostic tests:

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

Network Topologies

The Cisco ONS 15530 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 Planning Guide](#).

Standards Compliance

For information on standards compliance for the Cisco ONS 15530, refer to the [Regulatory Compliance and Safety Information for the Cisco ONS 15500 Series](#) publication.



Before You Begin

This chapter provides basic information about the Cisco ONS 15530. This chapter includes the following topics:

- [About the CLI, page 2-1](#)
- [About Cisco IOS Command Modes, page 2-1](#)
- [Interface Naming Conventions, page 2-4](#)
- [Configuration Overview, page 2-20](#)



Note

To ensure the installed Cisco IOS software supports your hardware and provides the software features you wish to use, see the [“New and Changed Information” section on page xiii](#). Also refer to the “Hardware Supported” section and “Feature Set” section of the latest release notes for the Cisco ONS 15530.

About the CLI

You can configure the Cisco ONS 15530 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 15530 through the console port or one of the TTY lines. By default, the terminal is configured to a basic configuration, which should work for most terminal sessions.

About Cisco IOS Command Modes

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

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

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

**Note**

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

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

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

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

Table 2-1 Frequently Used IOS Command Modes

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

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

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

1. Automatic Protection Switching

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

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

Listing Cisco IOS Commands and Syntax

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

```
Switch> ?
```

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

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

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

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

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

**Tips**

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

This section describes the interfaces and the interface naming conventions for each type of card supported by the Cisco ONS 15530.

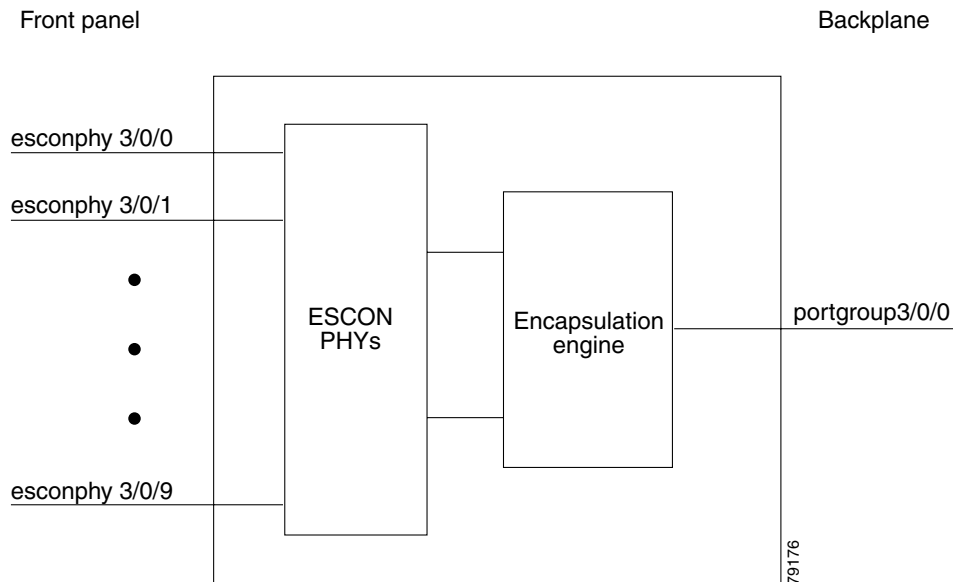
ESCON Aggregation Card Interfaces

The ESCON aggregation card has two types of interfaces:

- Esconphy interfaces
- Portgroup interfaces

Figure 2-1 shows the interfaces for the ESCON aggregation card.

Figure 2-1 ESCON Aggregation Card Interfaces



Esconphy Interfaces

The esconphy interfaces are located on the front panel of the ESCON aggregation cards. Each ESCON aggregation card has 10 esconphy interfaces. The ESCON aggregation card aggregates the signals from the esconphy interfaces into a single 2.5-Gbps signal and sends it to the portgroup interface on the backplane side of the card. The esconphy is an uncolored interface that carries ESCON physical layer signals. This interface does not terminate layer 2 or layer 3 protocol operations.

The naming convention for the esconphy interfaces on the ESCON aggregation card is as follows:

esconphy *slot/subcard/port*

Portgroup Interfaces

This logical interface represents the aggregation of multiple packet streams from the client side esconphy interfaces. The result is a 2.5-Gbps aggregate packet stream. The portgroup interface connects the interfaces on the front panel to the switch fabrics. A logical interface representing the aggregation of up to 10 ESCON client signals.

The naming convention for the portgroup interfaces is as follows:

portgroup *slot/subcard/port*

Each ESCON aggregation card has only one portgroup interface.

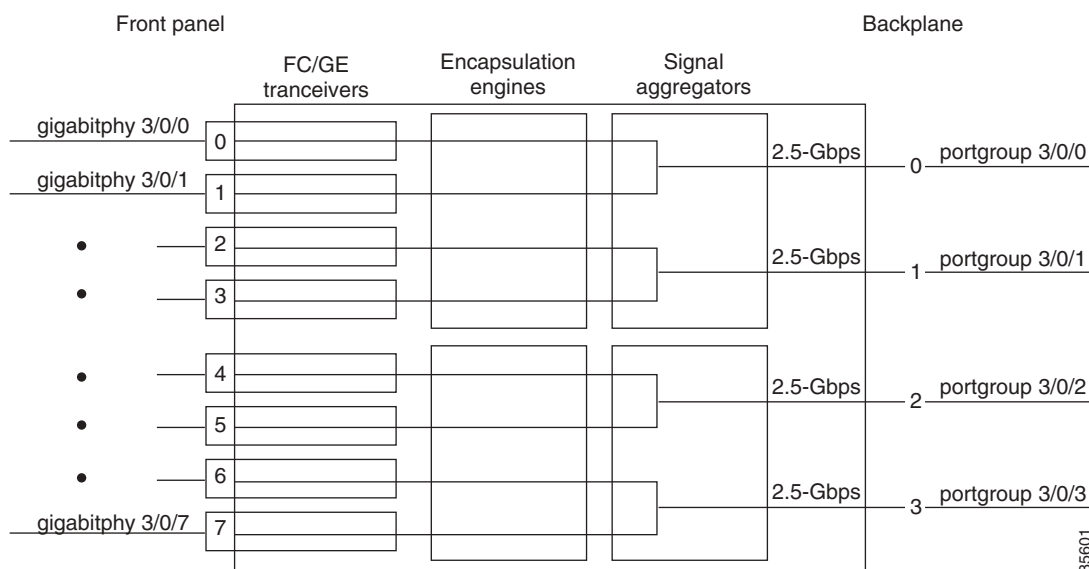
8-Port FC/GE Aggregation Card Interfaces

The 8-port FC/GE aggregation card has two types of interfaces:

- Gigabitphy interfaces
- Portgroup interfaces

Figure 2-2 shows the interfaces for the 8-port FC/GE aggregation card.

Figure 2-2 8-Port FC/GE Aggregation Card Interfaces



85601

Gigabitphy Interfaces

The gigabitphy interfaces are located on the front panel of the 8-port FC/GE aggregation cards. Each 8-port FC/GE aggregation card uses eight individually programmable SFPs for the gigabitphy interfaces. The 8-port FC/GE aggregation card aggregates the signals from adjoining pairs of gigabitphy interfaces (0 and 1, 2 and 3, 4 and 5, and 6 and 7, see [Figure 2-2](#)) into a four 2.5-Gbps signals and sends them to the portgroup interfaces on the backplane side of the card.

The naming convention for the gigabitphy interfaces on the 8-port FC/GE aggregation card is as follows:

gigabitphy *slot/subcard/port*

Portgroup Interfaces

This logical interface represents the aggregation of multiple packet streams from the client side gigabit interfaces. The result is a 2.5-Gbps aggregate packet stream. The portgroup interface connects the interfaces on the front panel to the switch fabrics. A logical interface representing the aggregation of up to two FC or GE client signals.

The naming convention for the portgroup interfaces is as follows:

portgroup *slot/subcard/port*

Each 8-port FC/GE aggregation card has four portgroup interfaces.

2.5-Gbps ITU Trunk Card Interfaces

The 2.5-Gbps ITU trunk cards have four types of interfaces:

- Ethernetdcc interfaces
- Wavethernetphy interfaces
- Wavepatch interfaces

[Figure 2-3](#) shows the interfaces for the splitter 2.5-Gbps ITU trunk card. [Figure 2-4](#) shows the interfaces for the nonsplitter 2.5-Gbps ITU trunk card.

Figure 2-3 Splitter 2.5-Gbps ITU Trunk Card Interfaces

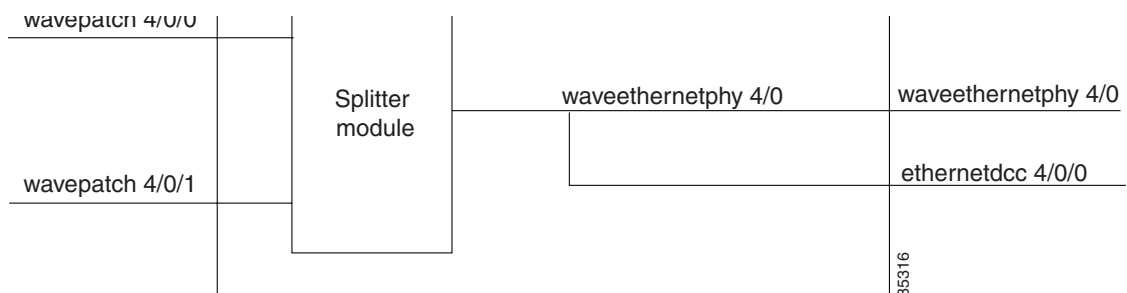
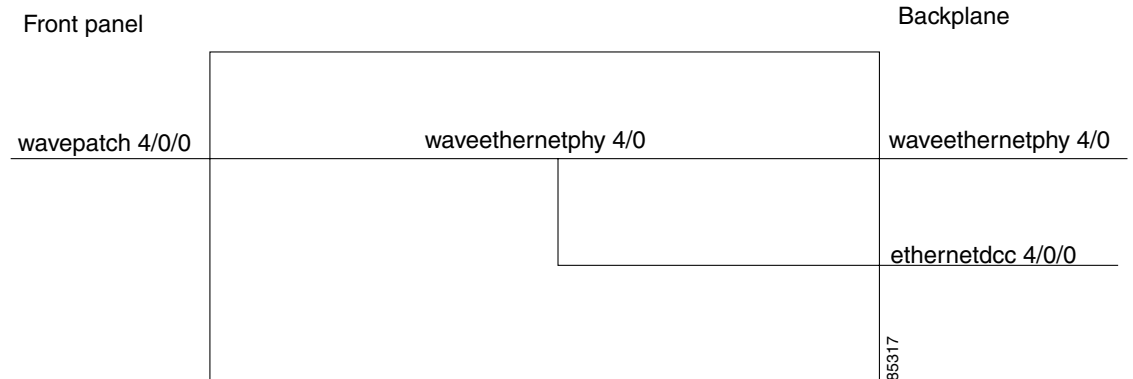


Figure 2-4 Nonsplitter 2.5-Gbps ITU Trunk Card Interfaces

Ethernetdcc Interfaces

The ethernetdcc interfaces provide the communication path for the in-band message channel OAM messages between the 2.5-Gbps ITU trunk card and the CPU switch modules. The ethernetdcc interface connects the switch fabrics to the waveethernetphy interface.

The naming convention for ethernetdcc interfaces is as follows:

ethernetdcc *slot/subcard/port*

Each card has one ethernetdcc interface.

Waveethernetphy Interfaces

The waveethernetphy interface corresponds to the laser on the 2.5-Gbps ITU trunk cards. The waveethernetphy interface connects to the wavepatch interface on the front panel. The waveethernetphy interface ITU signal carries a 2.5-Gbps physical layer signal. It does not terminate layer 2 or layer 3 protocol operations.

The naming convention for the waveethernetphy interfaces is as follows:

waveethernetphy *slot/subcard*

Each 2.5-Gbps ITU trunk card has one waveethernetphy interface.

Wavepatch Interfaces

The wavepatch interface is on the front panel of the 2.5-Gbps ITU trunk card. The waveethernetphy interface connects to the wavepatch interface on the backplane side. The mux/demux filter interface connects to the wavepatch interface on the front panel side.

A splitter 2.5-Gbps ITU trunk card has two wavepatch interfaces. A nonsplitter 2.5-Gbps ITU trunk card has only one wavepatch interface.

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

The naming convention for wavepatch interface is as follows:

wavepatch *slot/subcard/port*

10-Gbps ITU Trunk Card Interfaces

The 10-Gbps ITU trunk cards have four types of interfaces:

- Ethernetdccc interfaces
- Waveethernetphy interfaces
- Waveethernetphy subinterfaces
- Wavepatch interfaces

Figure 2-5 shows the interfaces for the splitter 10-Gbps ITU trunk card. Figure 2-6 shows the interfaces for the nonsplitter 10-Gbps ITU trunk card.

Figure 2-5 Splitter 10-Gbps ITU Trunk Card Interfaces

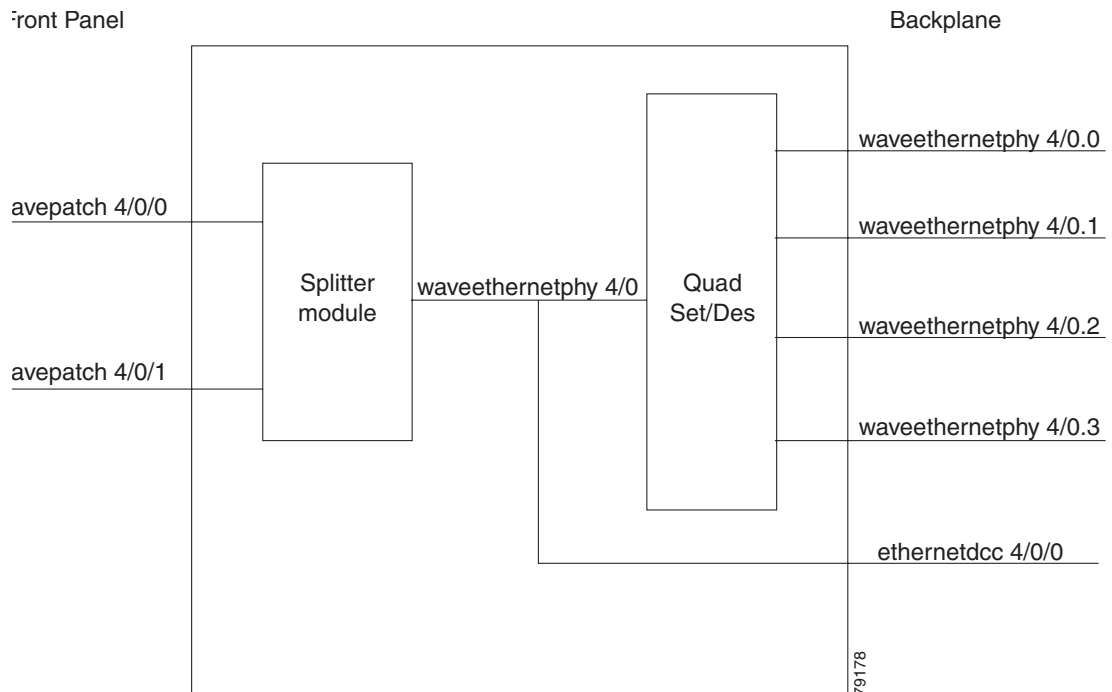
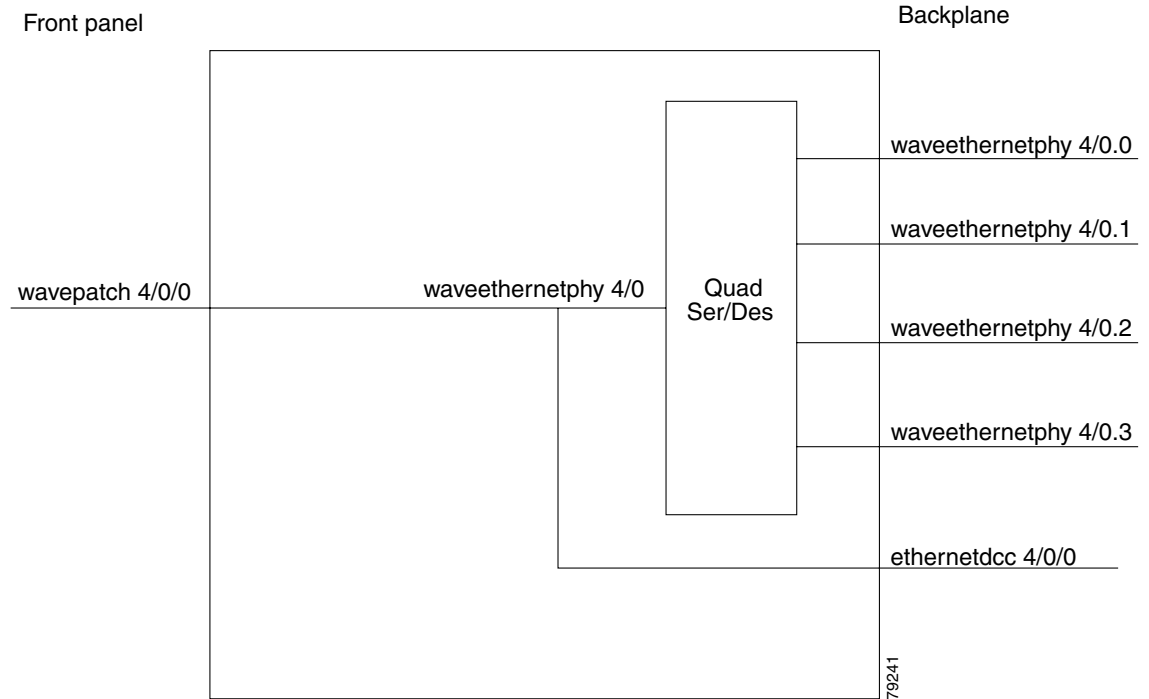


Figure 2-6 Nonsplitter 10-Gbps ITU Trunk Card Interfaces

Ethernetdcc Interfaces

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

The naming convention for ethernetdcc interfaces is as follows:

ethernetdcc *slot/subcard/port*

Each card has one ethernetdcc interface.

Waveethernetphy Interfaces

The waveethernetphy interfaces correspond to the laser on the 10-Gbps ITU trunk cards. The waveethernetphy interface connects the four waveethernetphy subinterfaces on the backplane side of the 10-Gbps ITU trunk card to the wavepatch interface on the front panel. The waveethernetphy interface ITU signal carries up to four 2.5-Gbps physical layer signals. It does not terminate layer 2 or layer 3 protocol operations.

The naming convention for the waveethernetphy interfaces is as follows:

waveethernetphy *slot/subcard*

Each 10-Gbps ITU trunk card has one waveethernetphy interface.

Waveethernetphy Subinterfaces

The waveethernetphy subinterfaces are located on the backplane side of the 10-Gbps ITU trunk cards. The waveethernetphy interface connects the switch fabric to the waveethernetphy interface. Each waveethernetphy subinterface can handle 2.5 Gbps of data traffic.

The naming convention for the waveethernetphy subinterfaces is as follows:

waveethernetphy *slot/subcard.subinterface*

Each 10-Gbps ITU trunk card has four waveethernetphy subinterfaces.

Wavepatch Interfaces

The wavepatch interfaces are on the front panel of the 10-Gbps ITU trunk card. The waveethernetphy interfaces connect to the wavepatch interfaces on the backplane side. The mux/demux filter interfaces connect to the wavepatch interface on the front panel side.

A splitter 10-Gbps ITU trunk card has two wavepatch interfaces. A nonsplitter 10-Gbps ITU trunk card has only one wavepatch interface.

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

The naming convention for wavepatch interfaces is as follows:

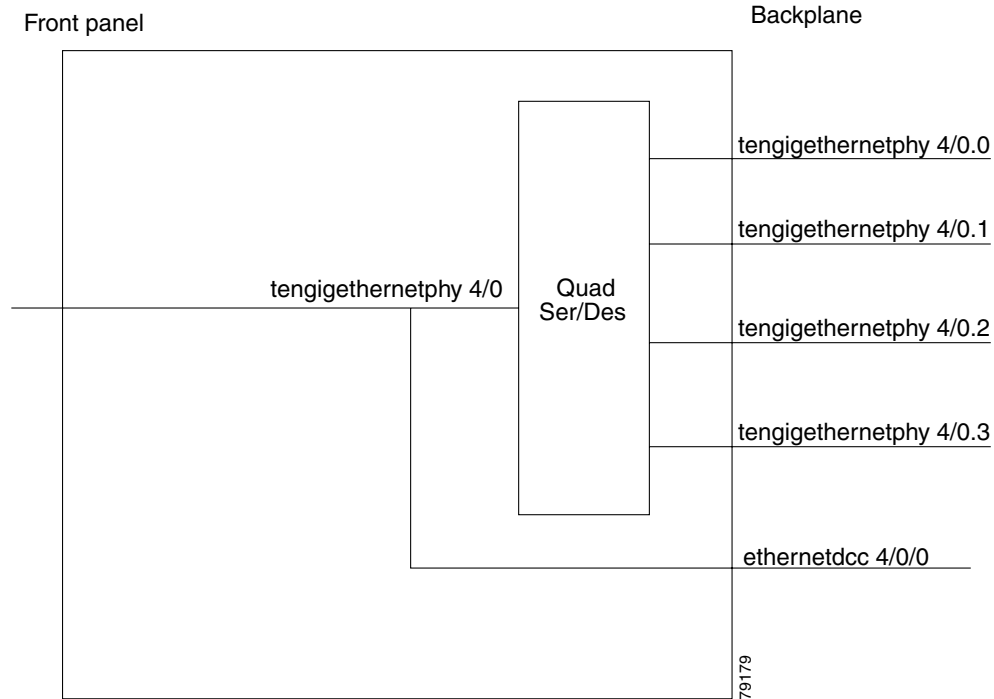
wavepatch *slot/subcard/port*

10-Gbps Uplink Card Interfaces

The 10-Gbps uplink cards have three types of interfaces:

- Ethernetdcc interfaces
- Tengigethernetphy interfaces
- Tengigethernetphy subinterfaces

Figure 2-7 shows the interfaces for the 10-Gbps uplink card.

Figure 2-7 10-Gbps Uplink Card Interfaces

Ethernetdccc Interfaces

The in-band message channel OAM messages for inband management are sent and received by the CPU switch module through the ethernetdccc interfaces. The ethernetdccc interface connects to the switch fabrics on the backplane side and the waveethernephy interface on the front panel side.

The naming convention for ethernetdccc interfaces is as follows:

ethernetdccc *slot/subcard/port*

Each 10-Gbps uplink card has one ethernetdccc interface.

Tengigethernephy Interfaces

The tengigethernephy interfaces correspond to the laser on the 10-Gbps uplink cards. The tengigethernephy interface connects to the tengigethernephy subinterface on the backplane side of the 10-Gbps uplink card and to the wavepatch interface on the front panel side. This is an uncolored interface that carries 10-Gigabit Ethernet. This interface does not terminate Layer 2 or Layer 3 protocol operations.

The naming convention for the tengigethernephy interfaces is as follows:

tengigethernephy *slot/subcard*

Each 10-Gbps uplink card has one tengigethernephy interface.

Tengigethernephy Subinterfaces

The tengigethernephy interfaces are the backplane interfaces on the 10-Gbps uplink cards. The tengigethernephy interface connects to the switch fabric.

The naming convention for the tengigethernetphy subinterfaces is as follows:

tengigethernetphy *slot/subcard.subinterface*

Each 10-Gbps uplink card has four tengigethernetphy subinterfaces.

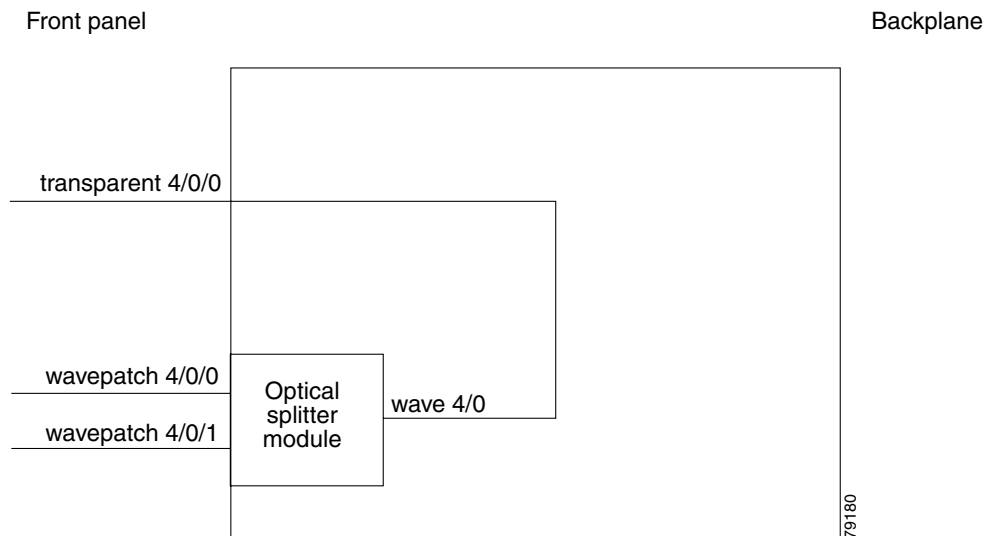
Transponder Line Card Interfaces

The transponder line cards have three types of interfaces:

- Transparent interfaces
- Wave interfaces
- Wavepatch interfaces

Figure 2-8 shows the interfaces for the transponder line card.

Figure 2-8 Transponder Line Card Interfaces



Transparent Interfaces

The transparent interfaces are located on the front panel of the transponder line cards. 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 transponder line card.

The naming convention for the transparent interfaces is as follows:

transparent *slot/subcard/port*

Each transponder line card has one transparent interface.

Wave Interfaces

The wave interface corresponds to the laser on the transponder line card that generates the channel. The wave interface electrically connects to the transparent interface on the front panel and optically connects to two wavepatch interfaces on a splitter card, or to one wavepatch interface on a nonsplitter card, on the ITU side.

The naming convention for wave interfaces is as follows:

wave *slot/subcard*

Each transponder line card has one wave interface.

Wavepatch Interfaces

The wavepatch interface is the interface on the front panel that connects to the filter interfaces on the OADM modules. The wave interfaces on the backplane side of the transponder line cards connect to the wavepatch interfaces.

Splitter transponder line cards have two wavepatch interfaces. Nonsplitter transponder line cards have only one wavepatch interface.

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*

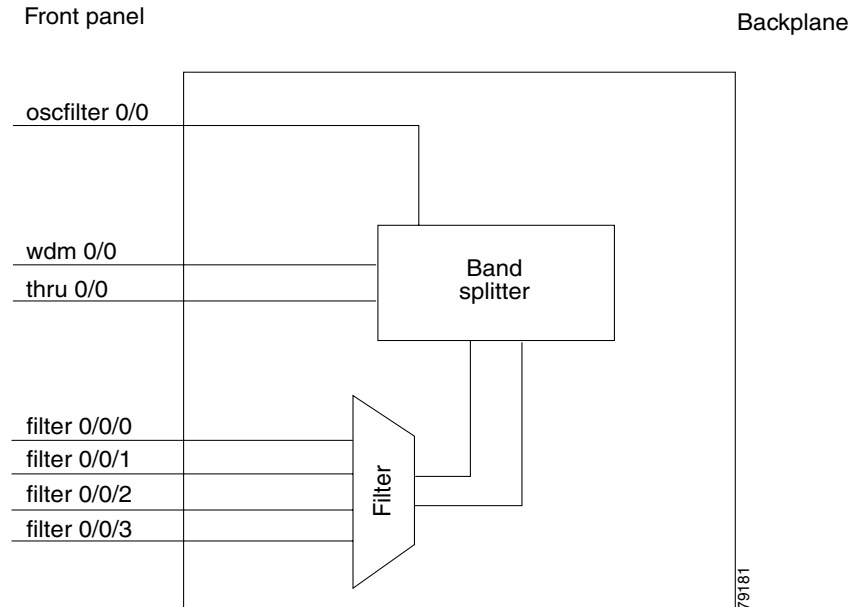
OADM Module Interfaces

The OADM modules can have four types of interfaces:

- Filter interfaces
- Oscfilter interfaces
- Wdm interfaces
- Thru interfaces

Figure 2-9 shows the interfaces for the OADM module.

Figure 2-9 OADM Module Interfaces



Filter Interfaces

The filter interface connects to a wavepatch interface on either a transponder line card, a 2.5-Gbps ITU trunk card, or a 10-Gbps ITU trunk card. Each filter interface corresponds to an individual wavelength filter. The filter interface connects a wavepatch interface to a wdm interface on the same OADM module.

The naming convention for filter interfaces is as follows:

filter *slot/subcard/port*

Each OADM module has four filter interfaces.

Oscfilter Interfaces

The OADM modules can support an optional OSC with an oscfilter interface. This interface connects to the wave interface on an OSC card.

The naming convention for the OSC interface on an OADM module is as follows:

oscfiler *slot/subcard*

Wdm Interfaces

The wdm interface is the interface on the OADM 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) on the front panel of an OADM module. The wdm interface connects either to a wdm interface on another network node, or to a thru interface on an OADM module on a different chassis in the same network node.

The naming convention for wdm interfaces is as follows:

wdm *slot/subcard*

Thru Interfaces

The thru interface is the interface on the OADM module that sends the DWDM signal to, or receives it from, another OADM module without altering it. It represents the pairs of fibers (Tx and Rx) on the front panel of an OADM module. The thru interface connects to the thru interface on the OADM module in the other subslot on the same chassis, or to a wdm interface on an OADM module on another chassis in the same network node.

The naming convention for thru interfaces is as follows:

thru *slot/subcard*

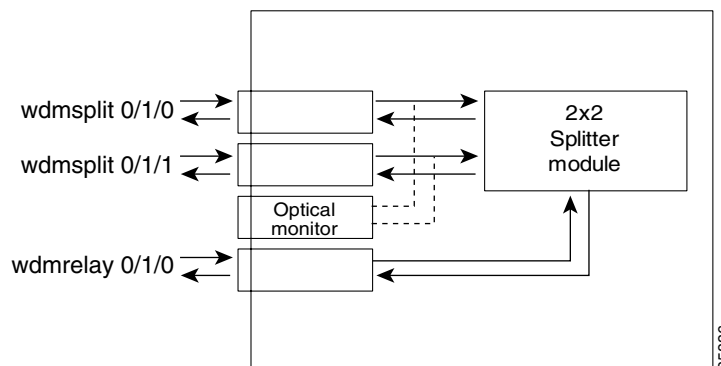
PSM Interfaces

The PSM (protection switch module) provides trunk fiber protection on the Cisco ONS 15530. The PSM has two types of interfaces:

- Wdmrelay interfaces
- Wdmsplit interfaces

Figure 2-10 shows the interfaces for the PSM.

Figure 2-10 PSM Interfaces



Wdmrelay Interfaces

The wdmrelay interface is a passive interface that represents a pair of fibers and connects the PSM to the wdm interface on the OADM module.

The naming convention for wdmrelay interfaces is as follows:

wdmrelay *slot/subcard/port*

Wdmsplit Interfaces

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

The naming convention for wdmsplit interfaces is as follows:

wdmsplit *slot/subcard/port*

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

OSC Card Interfaces

The optional OSC provides out-of-band management communications among the Cisco ONS 15530 systems in a network. The OSC is separate from the 32 data channels. The OSC card has one interface, the wave interface.

Wave Interfaces

The wave interface corresponds to the laser on the OSC card that generates the channel. The shelf can have up to two OSCs in the OSC motherboard, one per OADM module.

The naming convention for the OSC interface on an OADM module is as follows:

wave slot/subcard

CPU Switch Module Interfaces

The CPU switch modules have two types of interfaces:

- NME (network management Ethernet) interfaces
- Auxiliary port interfaces

NME Interfaces

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

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

**Note**

Network management system sessions and Telnet sessions are allowed on the NME interface on the active CPU switch module (`fastethernet 0`) but not allowed on the NME interface on the standby CPU switch module (`fastethernet-sby 0`).

Auxiliary Port Interfaces

Each CPU switch module has an auxiliary port interface. You can use this interface for modem connections. This interface is named `aux 0`. The DUART provides two UART channels, both of which connects to an RJ-45 connector on the front panel as the console and auxiliary ports. Typically, the console port connects to a console for configuring, controlling, or debugging the CPU switch module.

WB-VOA Card Interfaces

WB-VOA (wide-band variable optical attenuator) modules have two types of interfaces:

- Voain interfaces
- Voaout interfaces

Figure 2-11 shows the interfaces for the single WB-VOA module.

Figure 2-11 Single WB-VOA Module Interfaces

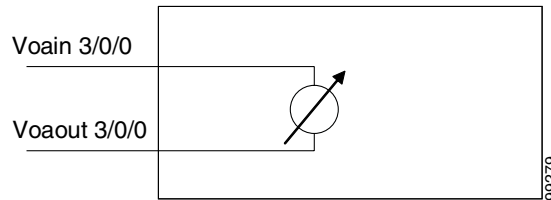
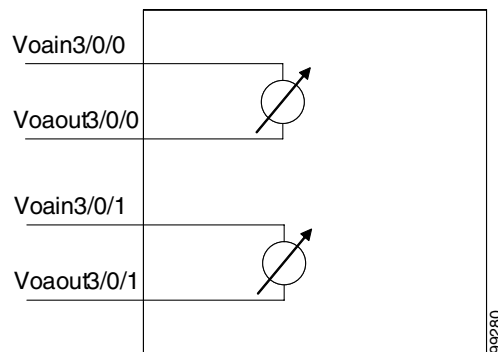


Figure 2-12 shows the interfaces for the dual WB-VOA module.

Figure 2-12 Dual WB-VOA Module Interfaces



Voain Interfaces

The voain interface is the input interface on a WB-VOA module. It accepts the signal to be attenuated.

The naming convention for the voain interface on a VOA card is as follows:

voain *slot/subcard/port*

Voaout Interfaces

The voaout interface is the output interface on a WB-VOA module. It transmits the attenuated signal.

The naming convention for the voaout interface on a VOA module is as follows:

voaout *slot/subcard/port*

PB-OE Module Interfaces

PB-OE (per-band optical equalizer) modules have four types of interfaces:

- Vofilterin interfaces and subinterfaces
- Vofilterout interfaces
- Voabypassin interfaces
- Voabypassout interfaces

Figure 2-13 shows the interfaces for the single PB-OE module.

Figure 2-13 Single PB-OE Module Interfaces

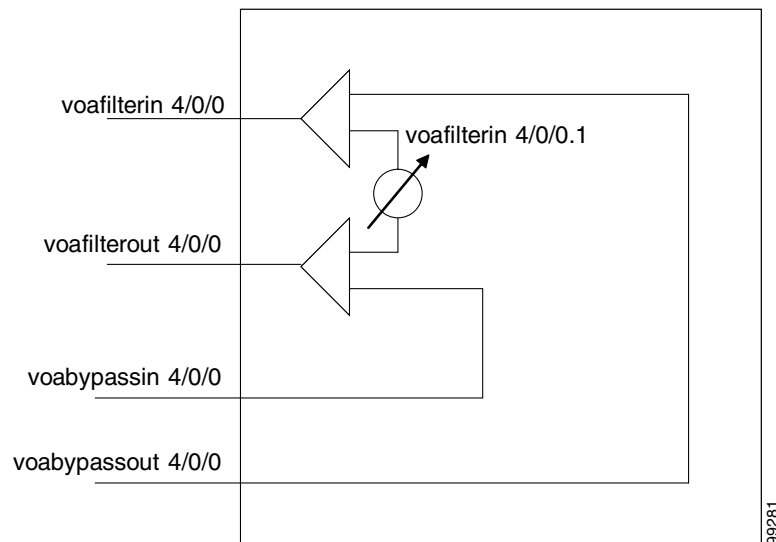
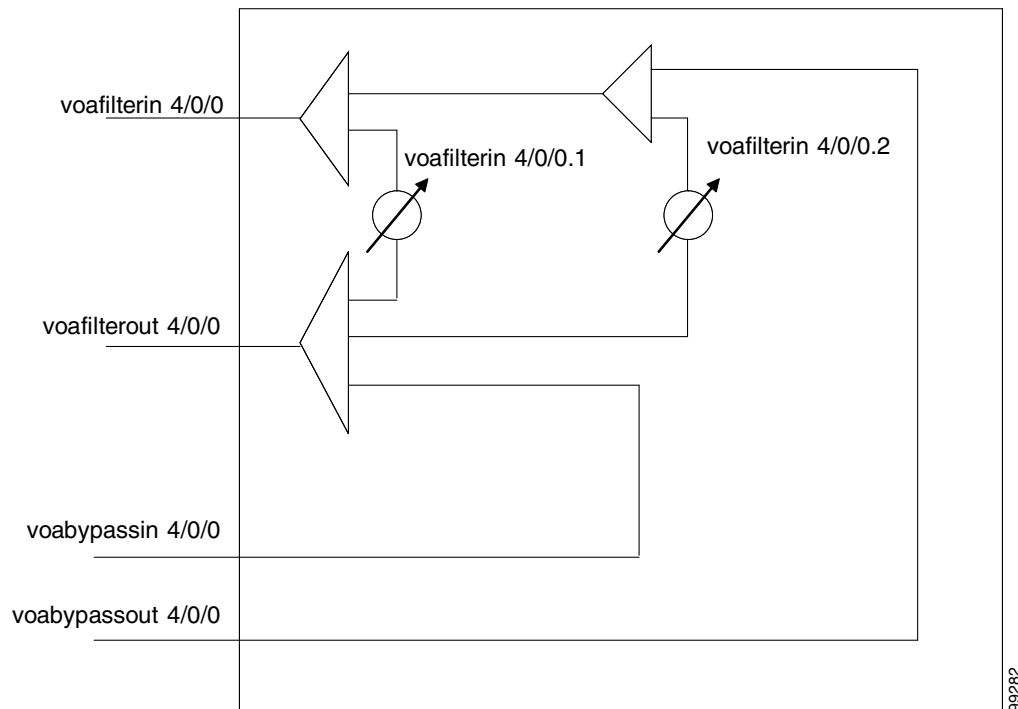


Figure 2-14 shows the interfaces for the dual PB-OE module.

Figure 2-14 Dual PB-OE Module Interfaces



Voafilterin Interfaces

The voafilterin interface identifies the physical port on the PB-OE that accepts the incoming DWDM signal for power equalization.

The naming convention for the voafilterin interface on a PB-OE module is as follows:

voafilterin *slot/subcard/port*

Voafilterin Subinterfaces

The voafilterin subinterface identifies the attenuator within the PB-OE module.

The naming convention for the voafilterin interface on a PB-OE module is as follows:

voafilterin *slot/subcard/port.subinterface*

Single band PB-OE modules have one voafilterin subinterface. Dual band PB-OE modules have two voafilterin subinterfaces.

Voafilterout Interfaces

The voafilterout interface sends the DWDM signal to the EDFA (erbium-doped fiber amplifier) or the next node in the network topology.

The naming convention for the voafilterout interface on a PB-OE module is as follows:

voafilterout *slot/subcard/port*

Voabypassout Interfaces

The voabypassout interface carries that portion of the signal not attenuated by the PB-OE module. This interface connects to another VOA module input interface (either a voain interface or a voafilterin interface) where the signal is further attenuated.

The naming convention for the voabypassout interface on a PB-OE module is as follows:

voabypassout *slot/subcard/port*

Voabypassin Interfaces

The voabypassin interface carries that portion of the signal attenuated on other modules. This interface connects to another VOA module output interface (either a voaout interface or a voafilterout interface) where the signal was attenuated.

The naming convention for the voabypassin interface on a PB-OE module is as follows:

voabypassin *slot/subcard/port*

Configuration Overview

To configure your Cisco ONS 15530 systems and network, perform the following steps:

-
- Step 1** Select line cards and modules to meet your requirements.
- For detailed information about the hardware components, refer to the [Cisco ONS 15530 Hardware Installation Guide](#). For detailed information on system planning and design, refer to the [Cisco ONS 15530 Planning Guide](#).
- Step 2** Insert the cards, motherboards, and CPU switch modules into the chassis.
- For detailed information on hardware configuration rules, refer to the [Cisco ONS 15530 Planning Guide](#).
- Step 3** Configure the NME ports on the active CPU switch module and on the standby CPU switch module, if present.
- For detailed information on configuring the NME port, see [Chapter 3, “Initial Configuration.”](#)
- Step 4** Connect the cards and modules with optical cables. Configure the patch connections with the CLI.
- For detailed information on cabling cards and modules, refer to the [Cisco ONS 15530 Planning Guide](#). For information on configuring cross connections, see the [“Configuring Cross Connections”](#) section on [page 4-8](#).
- Step 5** Configure aggregation flow identifier, the cross connections, and the patch connections for interfaces on all line cards, 2.5-Gbps ITU trunk cards, and 10-Gbps ITU trunk cards in the shelf. Also, configure the alarm thresholds and optical thresholds (optional).
- For detailed information on configuring these interfaces, see [Chapter 4, “Configuring ESCON Aggregation Card Interfaces,”](#) [Chapter 5, “Configuring 8-Port FC/GE Aggregation Card Interfaces,”](#) and [Chapter 7, “Configuring Trunk and Uplink Card Interfaces.”](#)
- Step 6** Configure either the protocol encapsulation or the clock rate for the client signal for all transponder line cards interfaces in the shelf. Also, enable protocol monitoring for supported protocols and configure the alarms thresholds (optional).
- For detailed information on transponder line card interface configuration, see [Chapter 6, “Configuring Transponder Line Card Interfaces.”](#)

- Step 7** Configure the VOA modules (optional).
For detailed information on VOA module interface configuration, see [Chapter 8, “Configuring VOA Module Interfaces.”](#)
- Step 8** Configure APS.
For detailed information on configuring APS, see [Chapter 10, “Configuring APS.”](#)
- Step 9** Configure CPU switch module redundancy.
For detailed information on CPU switch module redundancy, see the [“About CPU Switch Module Redundancy” section on page 3-11.](#)
- Step 10** Configure IP connectivity on the OSC or through 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 12-8.](#) For information on configuring IP connectivity via the in-band message channel, see the [“Configuring IP on Ethernetdcc Interfaces for the In-Band Message Channel” section on page 12-12.](#)
- Step 11** Configure CDP and the network topology.
For detailed information on network monitoring, see [Chapter 12, “Monitoring Your Network Topology.”](#)
-



Initial Configuration

This chapter describes how to configure the Cisco ONS 15530 so it can be accessed by other devices.

- [About the CPU Switch Module, page 3-1](#)
- [Starting Up the Cisco ONS 15530, page 3-2](#)
- [Using the Console Ports, NME Ports, and Auxiliary Ports, page 3-2](#)
- [About Passwords, page 3-3](#)
- [Configuring IP Access on the NME Interface, page 3-4](#)
- [Configuring the Host Name, page 3-6](#)
- [About NTP, page 3-7](#)
- [Configuring NTP, page 3-7](#)
- [Configuring Security Features, page 3-8](#)
- [About CPU Switch Module Redundancy, page 3-11](#)
- [Configuring CPU Switch Module Redundancy, page 3-15](#)
- [About the Software Configuration Register, page 3-24](#)
- [Changing the Software Configuration Register, page 3-28](#)
- [About Fan Failure Shutdown, page 3-29](#)
- [Configuring Fan Failure Shutdown, page 3-29](#)

About the CPU Switch Module

The CPU switch module provides intelligence to the Cisco ONS 15530. The CPU switch module supports SNMP (Simple Network Management Protocol) and many MIBs (Management Information Bases).

The Cisco ONS 15530 uses a QED RM7000 RISC processor. It runs at 78 MHz externally and at 234 MHz internally. It has a 64-bit multiplexed address and data bus with byte parity running at 78 MHz. It has separate internal L1 instruction and data caches of 16 KB each and internal L2 combined instruction/data cache of 256 KB.

The CPU switch modules also contains a 32 by 32 switch fabric that directs traffic from client cards to trunk cards. The switch fabric supports 2.5 Gbps data signals with 2R transparency.

The CPU switch module provides a slot on the front panel that accommodates a CompactFlash card. You can use the CompactFlash card for system image upgrades, FPGA image upgrades, statistics gathering, and other file system applications.

The Cisco ONS 15530 supports redundant operation with dual CPU switch modules. The CPU switch modules reside in slots 5 and 6, the sixth and seventh slots from the left as you face the chassis. For more information about redundancy, see the [“About CPU Switch Module Redundancy” section on page 3-11](#).

For more information on the CPU switch module, refer to the [Cisco ONS 15530 ESP Hardware Installation Guide](#).

Starting Up the Cisco ONS 15530

Before starting up the Cisco ONS 15530, you should verify the following:

- The system is set for the correct AC (or DC) power voltages.
Refer to the [Cisco ONS 15530 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 15530 Hardware Installation Guide](#) for instructions.

When you start up the Cisco ONS 15530, 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 CPU switch module.

Using the Console Ports, NME Ports, and Auxiliary Ports

You can configure the Cisco ONS 15530 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 15530 provides modem connection support. The following settings on the modem are required:

- Enable auto answer mode.
- Suppress result codes.
- Ensure auxiliary port terminal characteristics, such as speed, stop bits, and parity, match those of the modem.

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

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 that controls access to various commands and configuration modes. It contains from 1 to 25 uppercase and lowercase alphanumeric characters. Give the enable password only to users permitted to make configuration changes to the Cisco ONS 15530.

Enable Secret Password

The enable secret password is a secure, encrypted password. 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.

**Caution**

If you specify an encryption-type and then enter a clear text password, you will not be able to reenter enable mode. You cannot recover a lost password that has been encrypted by any method.

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 CPU switch module, named *fastethernet 0*, is the management interface that allows multiple, simultaneous Telnet or SNMP network management sessions.

You can remotely configure the Cisco ONS 15530 through the Fast Ethernet interface, but first you must configure an IP address so that the active CPU switch module is reachable. You can configure the NME interface two ways: 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 CPU switch module, *fastethernet-sby 0*, refer to the [Cisco ONS 15530 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 [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 5	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 6	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 7	Switch(config)# interface fastethernet 0 Switch(config-if)#	Enters interface configuration mode on interface <i>fastethernet 0</i> , the NME port on the active CPU switch module.
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)# no shutdown	Enables the interface.
Step 12	Switch(config-if)# exit Switch(config)#	Returns to global configuration mode.
Step 13	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 14	Switch(config-line)# password password	Specifies a password for Telnet sessions.
Step 15	Switch(config-line)# end Switch#	Returns to privileged EXEC mode.
Step 16	Switch# copy system:running-config nvram:startup-config	Saves the configuration changes to NVRAM.

The Cisco ONS 15530 NME interface should now be operating correctly.



Note

If a CPU switch module switchover occurs, you can use the same IP address to access the redundant CPU switch module after it becomes active.



Note

In a multiple shelf node configuration, perform these steps on the NME interfaces on all 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 15530. To configure the host name, perform the following steps:

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



Note

The host name is also synchronized with the standby CPU switch module. The host name prompt on the standby CPU switch module 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 ONS15530

```

```
ONS15530(config)# end
ONS15530# 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 15530 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 15530 supports the following Cisco IOS software security features:

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

Configuring AAA

This section describes the AAA features supported by the Cisco ONS 15530.

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 ATM switch router systems and send authentication requests to a central RADIUS server that contains all user authentication and network service access information. RADIUS is a fully open protocol, distributed in source code format, that can be modified to work with any security system currently available.

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

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

The following configuration tasks are optional:

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

Refer to the “[Configuring RADIUS](#)” chapter in the *Cisco IOS Security Configuration Guide*.

Configuring TACACS+

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

-
- Step 1** Use the **aaa new-model** global configuration command to enable AAA. AAA must be configured if you plan to use TACACS+. Refer to the “[AAA Overview](#)” chapter in the *Cisco IOS Security Configuration Guide*.
- Step 2** Use the **tacacs-server host** command to specify the IP address of one or more TACACS+ daemons. Use the **tacacs-server key** command to specify an encryption key that is used to encrypt all exchanges between the network access server and the TACACS+ daemon. This same key must also be configured on the TACACS+ daemon.

- Step 3** Use the **aaa authentication** global configuration command to define method lists that use TACACS+ for authentication. Refer to the “[Configuring Authentication](#)” chapter in the *Cisco IOS Security Configuration Guide*.
- Step 4** Use **line** and **interface** commands to apply the defined method lists to various interfaces. Refer to the “[Configuring Authentication](#)” chapter in the *Cisco IOS Security Configuration Guide*.
- Step 5** If needed, use the **aaa authorization** global command to configure authorization for the network access server. Unlike authentication, which can be configured per line or per interface, authorization is configured globally for the entire network access server. Refer to the “[Configuring Authorization](#)” chapter in the *Cisco IOS Security Configuration Guide*.
- Step 6** If needed, use the **aaa accounting** command to enable accounting for TACACS+ connections. Refer to the “[Configuring Accounting](#)” chapter in the *Cisco IOS Security Configuration Guide*.

Refer to the “[Configuring TACACS+](#)” chapter in the *Cisco IOS Security Configuration Guide*.

Configuring Traffic Filters and Firewalls

The Cisco ONS 15530 supports the traffic filter and firewall features provided by Cisco IOS.

Traffic filters provide basic traffic filtering capabilities with access control lists (also referred to as *access lists*). Access lists can be configured for all routed network protocols (IP, AppleTalk, and so on) to filter the packets of those protocols as the packets pass through a system. You can configure access lists on your Cisco ONS 15530 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.

Refer to the “[Traffic Filtering and Firewalls](#)” part in 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 CPU Switch Module Redundancy

The Cisco ONS 15530 supports fault tolerance by allowing the standby CPU switch module to take over if the active CPU switch module fails. This standby, or redundant, CPU switch module runs in hot-standby state. In hot-standby state, the standby CPU switch module is partially booted with Cisco IOS software, but no configuration is loaded.

At the time of a switchover from the active CPU switch module, the standby CPU switch module becomes active and loads the configuration as follows:

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

The former active CPU switch module then reloads and becomes the standby CPU switch module.



Note

If the standby CPU switch module 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 15530 is powered on, the two CPU switch modules arbitrate to determine which is the active CPU switch module and which is the standby CPU switch module. The following rules apply during arbitration:

- A newly inserted CPU switch module always comes up as the standby CPU switch module, except in cases where the newly inserted card is the only one present.
- If one of the CPU switch modules cannot boot its software image, the redundant CPU switch module boots as the active CPU switch module, allowing you to correct the situation manually.
- The primary route processor at the time the system is powered off continues as the primary when the system is powered on.
- If none of the above conditions is true, the CPU switch module in slot 6 becomes the active CPU switch module.

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

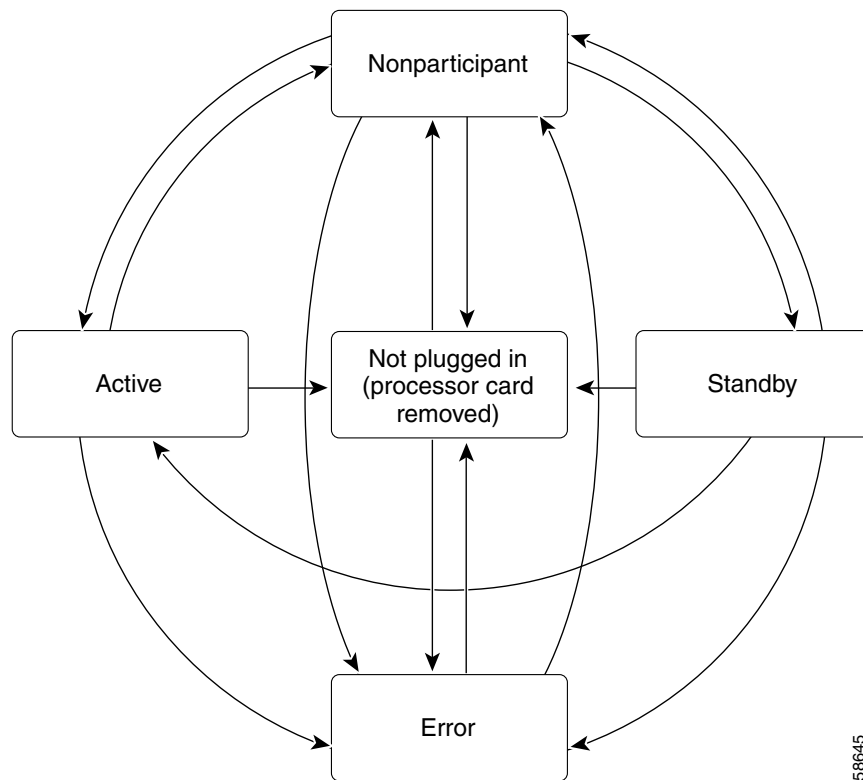
[Table 3-1](#) describes the five CPU switch module hardware states.

Table 3-1 CPU Switch Module Hardware States

State	Description
Active	Processor card is currently providing clock signals and control for all system cards. The active CPU switch module responds to the configured management IP address.
Standby	Processor card is partially booted in hot-standby state waiting to switch over when the active CPU switch module fails, when it is rebooted or removed, or when a manual switchover is requested.
Nonparticipant	Processor card is in ROMMON mode, or is in the process of booting, or has not yet reached the hot-standby state. Manual switchovers are rejected unless the force option is used.
Not plugged in	Processor card slot is empty.
Error	Processor card is present but either the interprocess arbitration interface is not functioning or the CPU switch module is not fully seated in the chassis slot.

Figure 3-1 shows the valid hardware transition states for a system with redundant CPU switch modules.

Figure 3-1 CPU Switch Module State Transition Diagram



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

Table 3-2 CPU Switch Module Software States

State	Description
Disabled	The standby CPU switch module is not yet running the system image or is in maintenance mode.
Standby cold	The standby CPU switch module is running the system image but has not begun to synchronize data from the active CPU switch module.
Standby hot	The standby CPU switch module has fully synchronized the configuration and other data from the active CPU switch module. It will remain in the hot-standby state until a switchover occurs.
Active	The CPU switch module 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 CPU switch modules are required.
- The CPU switch modules must have identical hardware configurations. This includes variables such as DRAM size, and so on.
- Both CPU switch modules must have the same functional image.
- Both CPU switch modules 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 CPU switch modules.
- Both CPU switch modules must be set to autoboot (a default setting).

If these requirements are met, the Cisco ONS 15530 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 15530 Software Upgrade Guide](#).

Conditions Causing a Switchover from the Active CPU Switch Module

The following conditions can cause a switchover from the active CPU switch module to the standby CPU switch module:

- The active CPU switch module is removed or swapped. When the CPU switch module functioning as the active CPU switch module is removed, the standby CPU switch module takes over. The Cisco ONS 15530 is nonredundant until a second CPU switch module is inserted.
- The active CPU switch module is rebooted. When a CPU switch module functioning as the active CPU switch module is rebooted, it relinquishes its active role if the standby CPU switch module has reached the hot-standby state.
- The active CPU switch module fails. The standby CPU switch module takes over as the active CPU switch module, 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 CPU Switch Module Redundancy

This section describes how to configure CPU switch module redundancy for your Cisco ONS 15530.



Note

The initial default configuration will support CPU switch module redundancy and database synchronization with no manual configuration required.

Forcing a Switchover from Privileged EXEC Mode

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

Command	Purpose
redundancy switch-activity [force]	Causes a CPU switch module switchover. If the standby CPU switch module 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 CPU switch module (formerly the active CPU switch module) automatically boots until it reaches the hot-standby state.



Note

Data transmission through the system is not affected by a CPU switch module switchover.

Example

The following example shows how to manually cause a CPU switch module 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 CPU switch module to take over as the active CPU switch module ROM monitor mode. To force a switchover from ROM monitor mode, enter the following commands on the active CPU switch module CLI:

Command	Purpose
switchover	Causes a CPU switch module reset and switchover. The CPU switch module 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 CPU switch module switchover from ROM monitor mode:

<Information deleted>

```

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

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

Reset Reason Register = RESET_REASON_SW_NMI (0x4)

Reset type 0x2

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

Initializing TLB

Initializing cache

Initializing required TLB entries
Initializing main memory

SDRAM DIMM size 67108864

Sizing NVRAM

Initializing PCMCIA controller

Initializing SRC FPGA
CPU arbitration

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

rommon 1 >

```

Configuring Autoboot

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

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

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



Note

If the standby CPU switch module remains in ROM monitor mode, you can manually boot the CPU switch module 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 15530 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-15530 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/1thanvan/manopt-m0-mz"

cisco (QUEENS-CPU) processor with 98304K/32768KB 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:ons15530-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 CPU switch modules. In the event of a switchover, the new active CPU switch module 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 CPU switch modules, use the following privileged EXEC command on the active CPU switch module:

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 CPU switch modules. Automatic synchronization ensures that, when a switchover occurs, the standby CPU switch module has the most recent configuration information.

**Note**

By default, the Cisco ONS 15530 automatically synchronizes the running configuration and the startup configuration between the two CPU switch modules.

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 CPU switch module

To enable or disable the system to automatically synchronize the configurations on both CPU switch modules, perform the following steps on the active CPU switch module, 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 15530 to enter the redundancy maintenance mode. Configuration synchronizations and standby CPU switch module fault reporting are suppressed in maintenance mode. Upon exiting maintenance mode and reverting to redundant mode, the standby switch CPU switch module reboots 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 CPU switch module.

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

	Command	Purpose
Step 1	Switch(config)# redundancy	Enters redundancy configuration mode.
	Switch(config-red)#	
Step 2	Switch(config-red)# maintenance-mode	Configures the system in maintenance mode.

Example

The following example shows how to configure redundancy maintenance mode:

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

Displaying the CPU Switch Module Redundancy Configuration and Status

To display the CPU switch module 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 CPU switch modules and the software version that is running.
show redundancy running-config-file	Displays the running configuration file on the standby CPU switch module. Note This command is only available on a terminal connected to the standby CPU switch module.

Examples

The following example shows the CPU switch module 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-15530 Software(ONS15530-I-M),...
Image File:            bootflash:ons15530-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-15530 Software(ONS15530-I-M),...
Image File (on sby-CPU): bootflash:ons15530-i-mz.010727
Software Redundancy State: STANDBY HOT
Hardware State:        STANDBY
Hardware Severity:     0

```

The following example shows the CPU switch module capabilities:

```
Switch# show redundancy capability
```

CPU capability support

Active CPU	Sby CPU	Sby Compat	CPU capability description
48 MB	48 MB	OK	CPU DRAM size
16 MB	16 MB	OK	CPU PMEM size
512 KB	512 KB	OK	CPU NVRAM size
16 MB	16 MB	OK	CPU Bootflash size
4.6	4.6	OK	CPU hardware major.minor version
1.43	1.43	OK	CPU functional major.minor version

Linecard driver major.minor versions, (counts: Active=13, Standby=13)

Active CPU	Sby CPU	Sby Compat	Drv/Ch/F ID	Driver description
1.3	1.3	OK	0x1100/0/0	CPU with Switch Fabric
2.3	2.3	OK	0x1101/0/0	10 Port ESCON line card
2.1	2.1	OK	0x110A/0/0	8 Port GE-FC line card
3.1	3.1	OK	0x1105/0/0	2.5G Transparent line card
1.9	1.9	OK	0x1105/1/0	2.5G Transparent line card
3.1	3.1	OK	0x1109/0/0	2.5G Transparent line card
1.9	1.9	OK	0x1109/1/0	2.5G Transparent line card
Active CPU	Sby CPU	Sby Compat	Drv/Ch/F ID	Driver description
1.3	1.3	OK	0x1103/0/0	OSC line card
0.1	0.1	OK	0x1107/1/0	OSC daughter card
2.1	2.1	OK	0x1102/0/0	10G trunk card
1.0	1.0	OK	0x110B/0/0	2.5G trunk card
2.1	2.1	OK	0x1110/0/0	PSM wdm splitter
1.1	1.1	OK	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.

Sync client counts: Active=6, Standby=6

Active CPU	Sby CPU	Sby Compat	Cl ID	Redundancy Client description
ver 1-2	ver 1-2	OK	17	CPU Redundancy
ver 1-1	ver 1-1	OK	19	Interface Sync
ver 1-1	ver 1-1	OK	36	MetOpt Password Sync
ver 1-2	ver 1-2	OK	18	Online Diagnostics
ver 1-2	ver 1-2	OK	6	OIR Client
ver 1-1	ver 1-1	OK	27	metopt cm db sync

```

ackplane IDPROM comparison
Backplane IDPROM field      Match Local CPU          Peer CPU
-----
idversion                   YES    1                        1
magic                       YES    153                     153
card_type                   YES    4358                    4358
order_part_num_str         YES    PROTO-HAMPTON-CHASSIS
                                PROTO-HAMPTON-CHASSIS
description_str             YES    Prototype Hampton Backplane
                                Prototype Hampton Backplane
board_part_num_str         YES    73-6573-03              73-6573-03
board_revision_str         YES    02                      02
serial_number_str          YES    TBC055089              TBC055089
date_of_manufacture_str    YES    10/21/2001             10/21/2001
deviation_numbers_str      YES    N/A                     N/A
manufacturing_use          YES    0                        0
rma_number_str             YES
rma_failure_code_str       YES
oem_str                     YES    Cisco                   Cisco
clei_str                   YES    TBD                     TBD
snmp_oid_substr            YES    TBD                     TBD
schematic_num_str         YES    92-4568-03             92-4568-03
Backplane IDPROM field      Match Local CPU          Peer CPU
-----
hardware_major_version     YES    3                        3
hardware_minor_version     YES    1                        1
engineering_use_str        YES    LAB Prototype           LAB Prototype
crc16                      OK     52960                   10284
user_track_string          NO     hello PhyAlias test    AssetTag123
                                lab
diagst                     YES    ^A                       ^A
board_specific_revision     YES    1                        1
board_specific_magic_number YES    153                     153
board_specific_length      YES    56                      56
mac_address_block_size     YES    16                      16
mac_address_base_str       YES    00016447a240           00016447a240
cpu_number                  OK     0                        1
optical_backplane_type     YES    255                     255

```

The following example shows how to display the running configuration file on the standby CPU switch module:

```

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 CPU Switch Modules

To reload one or both of the CPU switch modules, use the following privileged EXEC commands on the active CPU switch module CLI:

Command	Purpose
redundancy reload peer	Reloads the standby CPU switch module.
redundancy reload shelf	Reloads both CPU switch modules in the shelf.

Example

The following example shows how to reload the standby CPU switch module:

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

Configuring Privileged EXEC Mode Access on the Standby CPU Switch Module

Access to privileged EXEC mode from the standby CPU switch module CLI can be enabled from the active CPU switch module CLI. This feature provides extra security for the Cisco ONS 15530 system.

To configure access to privileged EXEC mode on the standby CPU switch module, perform the following steps on the active CPU switch module 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 CPU switch module 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 CPU Switch Module Privileged EXEC Mode Status

To display the privileged EXEC mode access status on the standby CPU switch module, 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 CPU switch module:

```
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-15530 Software (ONS15530-I-M), Release 12.1(10)EV
Image File:                ons15530-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 the Software Configuration Register

The Cisco ONS 15530 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 3-4 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 3-4. For example, the value of 0x0101 is a combination of settings (bit 8 is 0x0100 and bits 00 through 03 are 0x0001).

Table 3-4 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 causes 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 3-5 shows the combined effect of bits 14 and 10.

Table 3-5 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 3-6](#) shows the bit settings for the four available rates. The factory-set default data transmission rate is 9600.

Table 3-6 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 3-7 describes the values for the boot field.

Table 3-7 Configuration Register Boot Field Values

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

Default System Boot Behavior

The factory default value for the configuration register on the Cisco ONS 15530 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 15530 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 <i>value</i> is a hexadecimal number preceded by 0x . See Table 3-4 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 15530 fan assembly is located at the bottom of the chassis and contains six individual fans and a fan controller board. The controller board monitors the status of each fan and reports the status to the CPU switch modules.

If a single fan fails, a minor alarm is reported to the CPU switch module. 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 CPU switch module.

If all six fans in the fan tray fail, the chassis will reach critical temperature after 4 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 the following cards:

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

In addition, the ITU lasers on the transponder line cards are powered off.

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



Caution

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



Caution

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

Configuring Fan Failure Shutdown

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

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



Note

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

Example

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

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

Displaying the Fan Tray Failure Shutdown Configuration

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

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

Example

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

```
Switch# show environment
```

```
Fan
```

```
---
```

```
Status:                Total Failure
```

→ Line card shutdown on fan failure:enabled

```

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

```

```

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

```

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



Configuring ESCON Aggregation Card Interfaces

This chapter describes how to configure the interfaces on 10-port ESCON aggregation cards.

This chapter includes the following sections:

- [About ESCON Signal Aggregation Support, page 4-1](#)
- [Configuring ESCON Aggregation Card Interfaces, page 4-3](#)
- [About Latency and Transmit Buffers, page 4-5](#)
- [Configuring Transmit Buffer Size, page 4-6](#)
- [About Cross Connections, page 4-7](#)
- [Configuring Cross Connections, page 4-8](#)
- [About Alarm Thresholds, page 4-9](#)
- [Configuring Alarm Thresholds, page 4-9](#)



Note

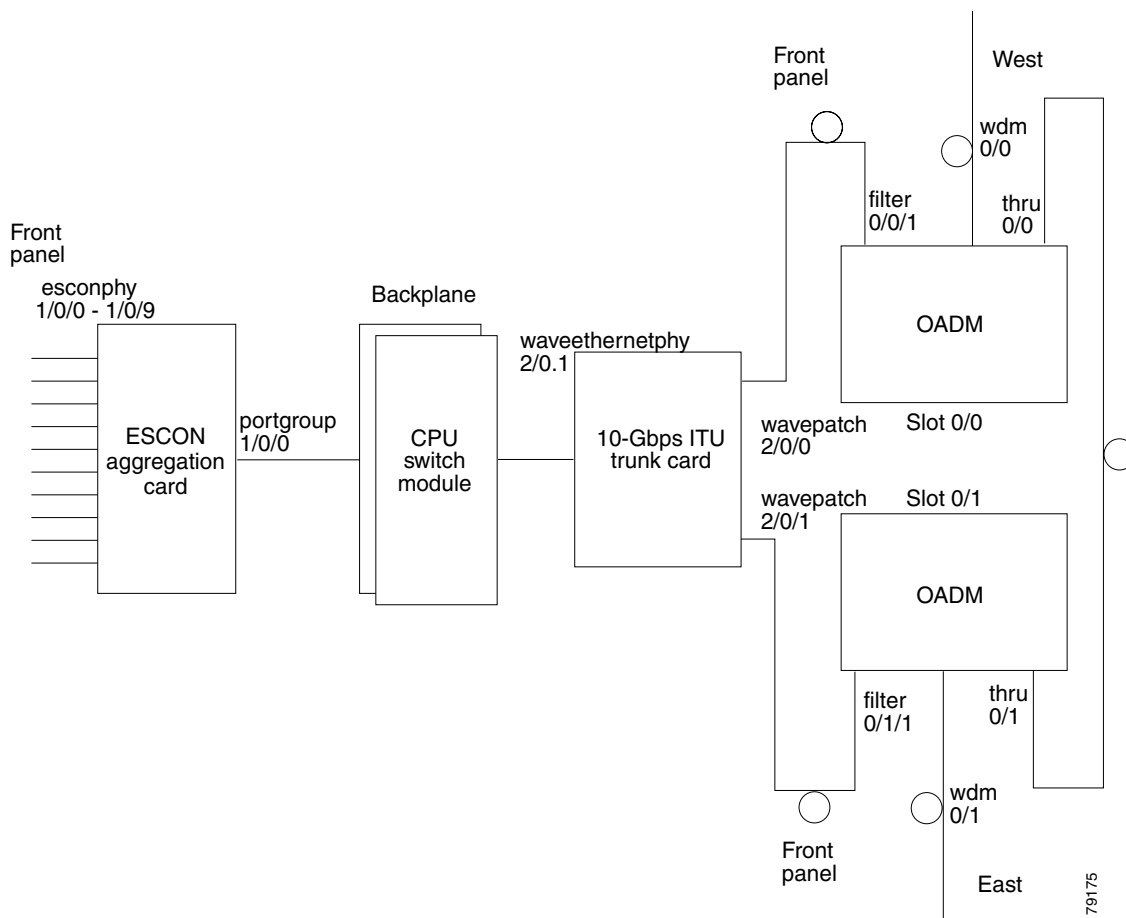
To ensure the installed Cisco IOS software supports your hardware and provides the software features you wish to use, see the [“New and Changed Information” section on page xiii](#). Also refer to the “Hardware Supported” section and “Feature Set” section of the latest release notes for the Cisco ONS 15530.

About ESCON Signal Aggregation Support

The ESCON aggregation card aggregates up to ten ESCON data streams into a single 2.5-Gbps signal, which is transmitted through the switch fabric to a 2.5-Gbps ITU trunk card, 10-Gbps ITU trunk card, or 10-Gbps uplink card. The ESCON aggregation card can be populated with up to ten SFP (small form-factor pluggable) optics.

[Figure 4-1](#) shows the path of an ESCON signal through the Cisco ONS 15530.

Figure 4-1 Interface Model for ESCON Aggregation





To configure ESCON support on the Cisco ONS 15530, perform the following steps:

-
- Step 1** Configure ESCON aggregation card interfaces.
 - Step 2** Configure 2.5-Gbps ITU trunk card interfaces, 10-Gbps ITU trunk card interfaces, or 10-Gbps uplink card interfaces as described in [Chapter 7, “Configuring Trunk and Uplink Card Interfaces.”](#)
 - Step 3** Configure cross connections.
 - Step 4** Configure alarm thresholds (optional).
 - Step 5** Configure patch connections.
-

Configuring ESCON Aggregation Card Interfaces

The ESCON aggregation card has two types of interfaces: ten esconphy interfaces on the client side and one portgroup interface on the trunk side. The primary feature to configure on the ESCON aggregation card is the in-band message channel flow identifier. The in-band message channel provides an encapsulation that uniquely identifies an ESCON signal when it is aggregated with the other ESCON signals.

To configure the ESCON aggregation card interfaces, perform the following tasks, starting in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface esconphy slot/0/port Switch(config-if)#	Specifies an interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# cdl flow identifier number	Configures the in-band message channel flow identifier. The range is 0 to 174. Note You must configure the other esconphy interface in the network that supports this signal with the same flow identifier.  Caution Use unique flow identifiers for each esconphy interface on the system. Duplicate flow identifiers might interfere with APS switchovers.
Step 3	Switch(config-if)# laser control forward enable	Enables forward laser control on the interface. The default for esconphy interfaces is enabled.
Step 4	Switch(config-if)# no shutdown	Enables the interface.
Step 5	Switch(config-if)# exit Switch(config)#	Returns to global configuration mode. Repeat Step 1 through Step 5 for the other esconphy interfaces on the ESCON aggregation card.
Step 6	Switch(config)# interface portgroup slot/0/0 Switch(config-if)#	Specifies an interface to configure and enters interface configuration mode.
Step 7	Switch(config-if)# cdl flow identifier reserve group-name	Configures the in-band message channel flow identifiers for all ten esconphy interfaces even if the SFPs are not populated. This step is required if the aggregated ESCON signal mixes with GE traffic on a 10-Gbps ITU trunk card. Note You must configure the other esconphy interface in the network that supports the signals with the same flow identifiers.  Caution Use unique flow identifiers for each esconphy interface on the system. Duplicate flow identifiers might interfere with APS switchovers.

**Note**

If traffic from an ESCON aggregation card mixes with GE traffic from an 8-port FC/GE aggregation card on the same 10-Gbps ITU trunk card, all ten esconphy interfaces must have flow control identifiers configured and those populated with SFPs must be enabled with the **no shutdown** command.

**Note**

When forward laser control is enable on an esconphy interface and a loss of light is detected on the port, the transmitter laser on the corresponding port on the remote node is turned off, regardless of the forward laser control configuration on the remote esconphy interface.

Example

The following example shows how to configure ESCON aggregation card interfaces:

```
Switch(config)# interface esconphy 10/0/0
Switch(config-if)# cdl flow identifier 100
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Displaying the ESCON Aggregation Card Interface Configuration

To display the configuration of ESCON aggregation card interfaces, use the following EXEC commands:

Command	Purpose
<code>show interfaces {esconphy portgroup} slot/subcard/port</code>	Displays the interface configuration.
<code>show cdl flow identifier</code>	Displays the in-band message channel flow identifiers for all interfaces on the system.

Examples

The following example shows how to display the configuration of an esconphy interface:

```
Switch# show interfaces esconphy 7/0/0
EsconPhy7/0/0 is administratively down, line protocol is down
  Forward laser control:On
  Threshold monitored for:None
  Received Frames:0
  Transmit Frames:0
  Code violation and running disparity error count( 8b10b cvrd):0
  CRC error count:0
  Egress Packet Sequence error count:0
  Egress Packet Indicated error count:0
  5 minute input rate 0 bits/sec, 0 frames/sec
  5 minute output rate 0 bits/sec, 0 frames/sec
  Transmit Buffer size is 16 bytes
  Hardware is escon_phy_port
```

The following example shows how to display the configuration of a portgroup interface:

```
Switch# show interfaces portgroup 10/0/0
Portgroup10/0/0 is up, line protocol is up
  Transmit Packets:171666543
  Received Packets:1559740251
  Code violation and running disparity error count(cvrd):93055574624
  Number of times SF threshold exceeded:1
  CRC error count:142890092
```



```

Number of times SF threshold exceeded:1
CDL HEC error count:142412666
Number of times SF threshold exceeded:1
SII Mismatch error count:473589
Protocol Mismatch error count:12
Transmit Buffer size is 16 bytes
Hardware is escon_portgroup

```

The following example shows how to display the flow identifiers on the system:

```

Switch# show cd1 flow identifier
Interface      Flow
Identifier
-----
Esco8/0/0      80
Esco8/0/1      81
Esco8/0/2      82
Esco8/0/3      83
Esco8/0/4      84
Esco8/0/5      85
Esco8/0/6      86
Esco8/0/7      87
Esco8/0/8      88
Esco8/0/9      89
Esco10/0/0     100
Esco10/0/1     255
Esco10/0/2     255
Esco10/0/3     255
Esco10/0/4     255
Esco10/0/5     255
Esco10/0/6     255
Esco10/0/7     255
Esco10/0/8     255
Esco10/0/9     255

```

About Latency and Transmit Buffers

The ESCON aggregation card adds latency to the transmission of ESCON traffic. [Table 4-1](#) shows the various configurations on the transmitting node and the ESCON latency values.



Note

The ESCON latency values have been determined by simulation and are approximate.

Table 4-1 Latency for ESCON Aggregation Cards

Traffic Mix on Transmitting Node	Maximum Added End-to-End Latency ¹			
	No GE	1518-Byte GE Packets	4470-Byte GE Packets	10,230-Byte GE Packets
ESCON only	8.5 microseconds			
ESCON and FC/FICON on the same 10-Gbps ITU trunk card	8.5 microseconds			
ESCON and GE only on the same 10-Gbps ITU trunk card		10 microseconds	12.5 microseconds	17 microseconds

1. The latency values are based on configuration of correct transmit buffer sizes as described in [Table 4-2](#).

A transmit buffer on the receiving node compensates for the packet jitter effects due to service multiplexing on the trunk. You must correctly configure the size of this transmit buffer to ensure that no buffer underflow or overflow occurs.

Configuring Transmit Buffer Size

To accommodate this latency on the receiving node, perform the following steps, starting in global configuration mode:


	Command	Purpose
Step 1	Switch(config)# interface <i>esconphy slot/0/port</i> Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# shutdown	Disables the interface.
Step 3	Switch(config-if)# tx-buffer size <i>bytes</i>	Configures the transmit buffer size. The default buffer size is 16 bytes. The range is 16 to 232. Note Changing the transmit buffer size on one <i>esconphy</i> interface changes it on all <i>esconphy</i> interfaces on the ESCON aggregation card.
		 Caution Issuing the tx-buffer size command might momentarily disrupt traffic through all <i>esconphy</i> interfaces on the card.
Step 4	Switch(config-if)# no shutdown	Enables the interface.

Table 4-2 provides the transmit buffer settings for various configurations.

Table 4-2 Latency for ESCON Aggregation Cards

Traffic Mix on Transmitting Node	Transmit Buffer Size (in Bytes) on the Receiving Node			
	No GE	1518-Byte GE Packets	4470-Byte GE Packets	10,230-Byte GE Packets
ESCON only	16 (default)			
ESCON and FC/FICON on the same 10-Gbps ITU trunk card	16 (default)			
ESCON and GE only on the same 10-Gbps ITU trunk card		24	72	168

Example

The following example shows how to configure the transmit buffer size on the receiving node:

```
Switch(config)# interface esconphy 3/0/2
Switch(config-if)# shutdown
Switch(config-if)# tx-buffer size 168
Switch(config-if)# no shutdown
```

Displaying Transmit Buffer Configuration

To display the transmit buffer configuration of an esconphy interface, use the following EXEC command:

Command	Purpose
<code>show interfaces esconphy slot0/port</code>	Displays the interface configuration.

Example

The following example shows how to display the transmit buffer configuration:

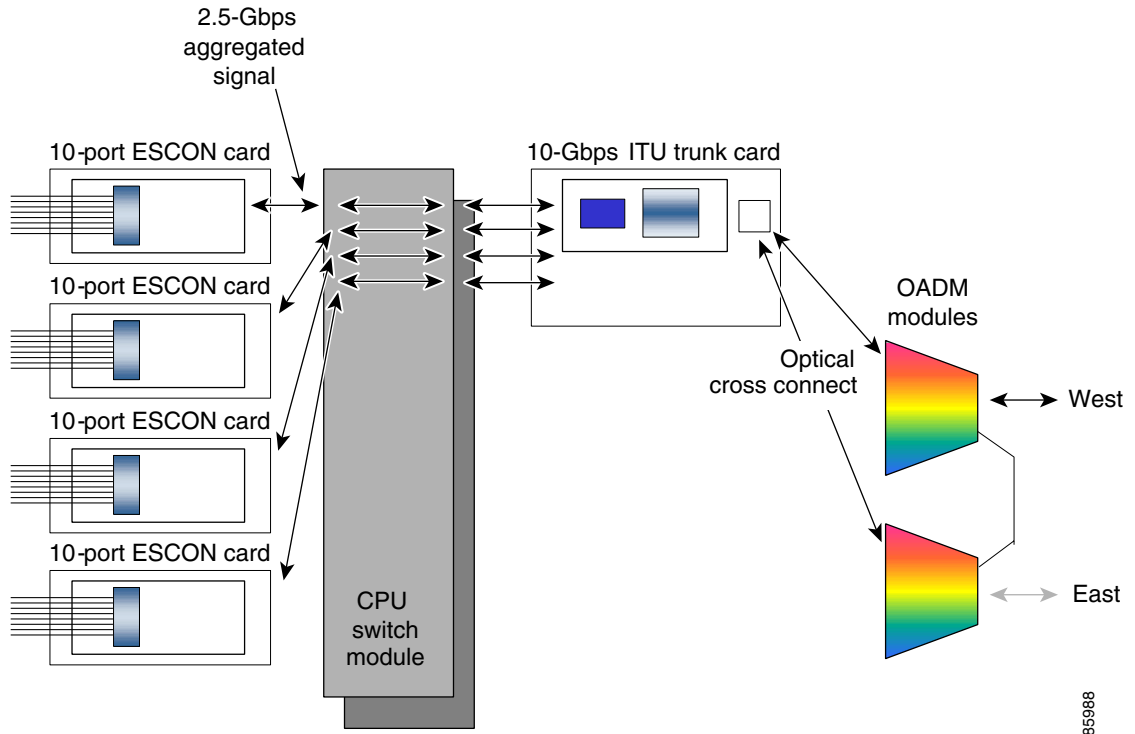
```
Switch# show interfaces esconphy 3/0/0
EsconPhy3/0/0 is administratively down, line protocol is down
  Forward laser control: On

  Configured threshold Group(s): all
  Threshold monitored for: CRC
  SF set value: 10e-8 (2 in 1 secs)
  SD set value: 10e-9 (1 in 5 secs)
  Received Frames: 0
  Transmit Frames: 0
  Code violation and running disparity error count( 8b10b cvrd): 0
  CRC error count: 0
  Number of times SF threshold exceeded: 0
  Number of times SD threshold exceeded: 0
  Egress Packet Sequence error count: 0
  Egress Packet Indicated error count: 0
  5 minute input rate 0 bits/sec, 0 frames/sec
  5 minute output rate 0 bits/sec, 0 frames/sec
→ Transmit Buffer size is 168 bytes
  Hardware is escon_phy_port
```

About Cross Connections

The client signal follows a path of interface optical cross connections through the Cisco ONS 15530. [Figure 4-2](#) shows an example of cross connections. Knowing the path of a signal through the shelf helps with system management and troubleshooting.

Figure 4-2 Optical Cross Connection Example



85988

Configuring Cross Connections

The aggregated signal from the ESCON aggregation cards passes through the switch fabric to the 2.5-Gbps ITU trunk card, 10-Gbps ITU trunk card, or the 10-Gbps uplink card. To establish a cross connection through the switch fabric, perform the following steps, beginning in global configuration mode:

Command	Purpose
Switch(config)# connect <i>interface1 interface2</i>	Creates a cross connection between two interfaces through the switch fabric.

Caution

If ESCON traffic mixes with GE traffic on a 10-Gbps ITU trunk card, be sure to assign flow identifiers to all `esconphy` interfaces, using either the `cdl flow identifier` command or the `cdl flow identifier reserved` command, and to enable the interfaces with the `no shutdown` command.

Example

The following example shows how to configure a cross connection between an ESCON aggregation card and a 2.5-Gbps ITU trunk card:

```
Switch(config)# connect portgroup 2/0/0 waveethernetphy 3/0
```

The following example shows how to configure a cross connection between an ESCON aggregation card and a 10-Gbps ITU trunk card:

```
Switch(config)# connect portgroup 2/0/0 waveethernetphy 3/0.1
```

The following example shows how to configure a cross connection between an ESCON aggregation card and a 10-Gbps uplink card:

```
Switch(config)# connect portgroup 2/0/0 tengigethernetphy 3/0.1
```

Displaying the Cross Connection Configuration

To display the cross connection configuration, use the following privileged EXEC command:

Command	Purpose
<code>show connect [edge intermediate [sort-channel interface <i>interface</i>]]</code>	Displays the signal cross connection configuration through the system.

Example

The following example shows the cross connections within a system for an ESCON signal:

```
Switch# show connect
Index Client Intf      Trunk Intf      Kind      C2TStatus  T2CliStatus
-----
15     Port3/0/0      WaveE8/0.1     Provisioned Up         Up
```

About Alarm Thresholds

You can configure thresholds on the ESCON aggregation card interfaces that issue alarm messages to the system if the thresholds are exceeded.

Every second, the monitoring facility updates the counters that correspond to the alarm thresholds. When the signal degrades, or fails entirely, the system issues alarms to the console. These alarms can help isolate failures in the system and in the network.

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

Configuring Alarm Thresholds

To configure alarm thresholds on the ESCON aggregation card, 2.5-Gbps ITU trunk card, 10-Gbps ITU trunk card, and 10-Gbps uplink card interfaces, perform the following steps, beginning in global configuration mode:

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

	Command	Purpose
Step 3	Switch(config-t-list)# threshold name {cvrd cdl hec crc sonet-sdh section cv tx-crc} {failure degrade} [index value] Switch(config-threshold)#	Specifies a threshold type to modify and enters threshold configuration mode.
Step 4	Switch(config-threshold)# value rate value	Specifies the threshold rate value. This value is the negative power of 10 (10 ⁻ⁿ).
Step 5	Switch(config-threshold)# description text	Specifies a description of the threshold. The default value is the null string. (Optional)
Step 6	Switch(config-threshold)# exit Switch(config-t-list)#	Returns to threshold list configuration mode. Repeat Step 3 through Step 6 to configure more thresholds in the threshold list.
Step 7	Switch(config-t-list)# exit Switch(config)#	Returns to global configuration mode.
Step 8	Switch(config)# interface interface Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 9	Switch(config-if)# threshold-group name	Configures the threshold list on the interface.

**Note**

When a threshold list is applied to one esconphy interface all esconphy interfaces on the ESCON aggregation card inherit that threshold list configuration.

Table 4-3 lists the threshold error rates in errors per second for ESCON signals.

Table 4-3 Threshold Values for Monitored Rates for ESCON Signals in Errors Per Second

Rate	ESCON CRC	ESCON CVRD
3	19999	20000
4	19999	20000
5	1999	2000
6	199	200
7	20	20
8	2	2
9	0.2	0.2

Example

The following example shows how to create an alarm threshold list and configure that list for ESCON aggregation card interfaces:

```
Switch# configure terminal
Switch(config)# threshold-list escon-counters
Switch(config-t-list)# threshold name crc degrade
Switch(config-threshold)# value rate 9
Switch(config-threshold)# exit
Switch(config-t-list)# threshold name crc failure
Switch(config-threshold)# value rate 7
```

```
Switch(config-threshold)# exit
Switch(config-t-list)# exit
Switch(config)# interface esconphy 3/0/0
Switch(config-if)# threshold-group escon-counters
```

Displaying the Alarm Threshold Configuration

To display the configuration of a threshold list and the threshold group for an esconphy interface, use the following EXEC commands:

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

Examples

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

```
Switch# show threshold-list escon-counters

Threshold List Name: escon-counters
Notification throttle timer : 5 (in secs)
Threshold name : CRC Severity : Degrade
Value : 10e-9
APS Trigger : Not set
Threshold name : CRC Severity : Failure
Value : 10e-7
APS Trigger : Not set
```

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

```
Switch# show interfaces esconphy 3/0/0
EsconPhy3/0/0 is up, line protocol is up
Signal quality: Good
Forward laser control: Off
Configured threshold Group: escon-counters
Threshold monitored for: CRC
SF set value: 10e-7 (20 in 1 secs)
SD set value: 10e-9 (1 in 5 secs)
Received Frames: 0
Transmit Frames: 0
Code violation and running disparity error count(cvrd): 0
Number of times SF threshold exceeded: 0
Number of times SD threshold exceeded: 0
CRC error count: 0
Number of times SF threshold exceeded: 0
Number of times SD threshold exceeded: 0
Egress Packet Sequence error count: 0
Egress Packet Indicated error count: 0
5 minute input rate 0 bits/sec, 0 frames/sec
5 minute output rate 0 bits/sec, 0 frames/sec
Hardware is escon_phy_port
```




Configuring 8-Port FC/GE Aggregation Card Interfaces

This chapter describes how to configure 8-port Fibre Channel/Gigabit Ethernet aggregation cards on the Cisco ONS 15530. This chapter includes the following sections:

- [About the 8-Port FC/GE Aggregation Card, page 5-1](#)
- [Configuring 8-Port FC/GE Aggregation Card Interfaces, page 5-3](#)
- [About Latency and Transmit Buffers, page 5-6](#)
- [Configuring Transmit Buffer Size for FC, FICON, and ISC, page 5-7](#)
- [About Cross Connections, page 5-9](#)
- [Configuring Cross Connections, page 5-10](#)
- [About Alarm Thresholds, page 5-11](#)
- [Configuring Alarm Thresholds, page 5-11](#)



Note

To ensure the installed Cisco IOS software supports your hardware and provides the software features you wish to use, see the [“New and Changed Information” section on page xiii](#). Also refer to the [“Hardware Supported” section](#) and [“Feature Set” section](#) of the latest release notes for the Cisco ONS 15530.

About the 8-Port FC/GE Aggregation Card

The 8-port FC/GE aggregation card uses SFP (small form-factor pluggable) optical transceivers to provide up to eight configurable client interfaces. Each interface can be configured in the CLI (command-line interface) for FC (Fibre Channel), FICON (fiber connection), GE (Gigabit Ethernet), or ISC-3 (InterSystem Channel) links compatibility mode traffic.

To configure the 8-port FC/GE aggregation card on the Cisco ONS 15530, perform the following steps:

- Step 1** Configure 8-port FC/GE aggregation card interfaces.
- Step 2** Configure 2.5-Gbps ITU trunk card interfaces, 10-Gbps ITU trunk card interfaces, or 10-Gbps uplink card interfaces as described in [Chapter 7, “Configuring Trunk and Uplink Card Interfaces.”](#)
- Step 3** Configure the transmission buffer size (optional; FC and FICON traffic only).
- Step 4** Configure cross connections.

Step 5 Configure alarm thresholds (optional).



Note

The MTU size in the 8-port FC/GE aggregation card is 10232 bytes.



Note

The Cisco IOS software only supports Cisco-certified SFP optics on the 8-port FC/GE aggregation card.

Protocol Monitoring

For GE traffic, the Cisco ONS 15530 monitors the following conditions on the 8-port FC/GE aggregation card:

- CVRD error counts
- Tx/Rx frame counts
- Tx/Rx byte counts
- Tx/Rx CRC errors
- Giant packet counts
- Runt packet counts
- 5 minute input/output rates

For FC and FICON traffic, the system monitors the following conditions on the 8-port FC/GE aggregation card:

- CVRD error counts
- Tx/Rx frame counts
- Tx/Rx byte counts
- Rx CRC errors
- Link failures
- Sequence protocol errors
- Invalid transmission words
- 5 minute input/output rates
- Loss of Sync
- Loss of Light

For ISC-3 compatibility mode traffic, the system monitors the following conditions on the 8-port FC/GE aggregation card:

- CVRD error counts
- Loss of Light

Support for FC Port Types

The 8-port FC/GE aggregation card supports the following FC port types, with or without the buffer credit distance extension feature enabled:

- B_port—bridge port
- E_port—expansion port
- F_port—fabric port
- N_port—node port
- TE_port—trunking E_port (Cisco MDS 9000 Family systems only)



Note

All of the above port topologies, except for TE_port, are point-to-point in Fibre Channel specifications.

Examples of valid topologies where you can put a Cisco ONS 15530 with an 8-port FC/GE aggregation card in the middle to extend distance include the following:

- E_Port <--> E_Port
- F_Port <--> N_Port
- N_Port <--> N_Port
- B_Port <--> B_Port
- TE_Port <--> TE_Port

Arbitrated loop topology is not supported by the 8-port FC/GE aggregation card. The arbitrated loop port types not supported include:

- NL_port—node loop port
- FL_port—fabric loop port
- EL_port—extension loop port

So any combination of above port types are not supported.

Configuring 8-Port FC/GE Aggregation Card Interfaces

The 8-port FC/GE aggregation card has two types of interfaces: eight gigabitphy interfaces on the client side and four portgroup interfaces on the trunk side.

To configure the 8-port FC/GE aggregation card interfaces, perform the following tasks, starting in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface gigabitphy slot/0/port Switch(config-if)#	Specifies an interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# encapsulation {fibrenchannel [ofc {enable disable}] ficon [ofc {enable disable}] gigabitethernet sysplex isc compatibility}	Configures the interface as either FC, FICON, GE, or ISC-3 compatibility mode. The default mode for OSC is disabled.

	Command	Purpose
Step 3	Switch(config-if)# cdl flow identifier <i>number</i>	Specifies the flow identifier for the signal. The range is 0 to 174.
Step 4	Switch(config-if)# laser control forward enable	Enables forward laser control on the interface. The default is disabled. (Optional)
Step 5	Switch(config-if)# flow control	Enables buffer credits when the interface is encapsulated for Fibre Channel traffic. The default is disabled. (Optional)
Step 6	Switch(config-if)# negotiation auto	Enables autonegotiation between the 8-port FC/GE aggregation card and the client equipment when the interface is encapsulated for Gigabit Ethernet traffic. The default is disabled. (Optional) Note The 8-port FC/GE aggregation card does not support end-to-end passthrough of the autonegotiation parameters.
Step 7	Switch(config-if)# no shutdown	Enables the interface.
Step 8	Switch(config-if)# exit Switch(config)#	Returns to global configuration mode. Repeat Step 1 through Step 8 for the other gigabitphy interfaces on the 8-port FC/GE aggregation card.

**Caution**

If ESCON traffic mixes with GE traffic on a 10-Gbps ITU trunk card, assign flow identifiers to all esconphy interfaces, using either the **cdl flow identifier** command or the **cdl flow identifier reserved** command, and enable the interfaces with the **no shutdown** command.

**Note**

When forward laser control is enable on an gigabitphy interface and a loss of light is detected on the port, the transmitter laser on the corresponding port on the remote node is turned off, regardless of the forward laser control configuration on the remote gigabitphy interface.

Example

The following example shows how to configure 8-port FC/GE aggregation card interfaces:

```
Switch(config)# interface gigabitphy 3/0/0
Switch(config-if)# encapsulation fibrechannel
Switch(config-if)# cdl flow identifier 30
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Displaying the 8-Port FC/GE Aggregation Card Interface Configuration

To display the configuration of 8-port FC/GE aggregation card interfaces, use the following EXEC command:

Command	Purpose
<code>show interfaces {gigabitphy portgroup} slot/subcard/port</code>	Displays the interface configuration.

Example

The following example shows how to display the configuration of a gigabitphy interface configured as GE:

```
Switch# show interfaces gigabitphy 2/0/0
GigabitPhy2/0/0 is up, line protocol is up
  Optical Transceiver:Single Mode
  Signal quality:Good
  Encapsulation:GigabitEthernet
  Time of last "encapsulation" change 00:47:39
  Forward laser control:Off
  Flow-identifier:20
  Loopback not set

  Configured threshold Group(s):txcrc-sf6
  Threshold monitored for:tx-crc
  SF set value:10e-6 (994 in 1 secs)
  Received Frames:39489
  Received Bytes:59233500
  Transmit Frames:39489
  Transmit Bytes:59233500
  Code violation and running disparity error count( 8b10b cvrd):0
  RX CRC errors:39489
  TX CRC errors:39489
  Giant Packets:0
  Runt Packets:0
  5 minute input rate 0 bits/sec, 0 frames/sec
  5 minute output rate 0 bits/sec, 0 frames/sec
  Transmit Buffer size is 256 bytes
  Hardware is gige_fc_phy_port
```

The following example shows how to display the configuration of a gigabitphy interface configured as FC:

```
Switch# show interfaces gigabitphy 2/0/1
GigabitPhy2/0/1 is down, line protocol is down
  Optical Transceiver:Single Mode
  Signal quality:Loss of light
  Encapsulation:Fibre channel   Rate:1G   Ofc:off
flow control:disabled
  Time of last "encapsulation" change 00:47:46
  Forward laser control:Off
  Flow-identifier:21
  Loopback not set

  Configured threshold Group(s):txcrc-sf3
  Threshold monitored for:tx-crc
  SF set value:10e-3 (83333 in 1 secs)
  Received Frames:0
  Received Bytes:0
  Transmit Frames:0
```

```

Transmit Bytes:0
Code violation and running disparity error count( 8b10b cvrd):0
RX CRC errors:0
Link Failures:0
Loss of Sync:0
Loss of Light:0
Sequence Protocol Error count:0
Invalid Transmission Word count:0
5 minute input rate 0 bits/sec, 0 frames/sec
5 minute output rate 0 bits/sec, 0 frames/sec
Transmit Buffer size is 256 bytes
Hardware is gige_fc_phy_port

```

The following example shows how to display the configuration of a portgroup interface:

```

Switch# show interfaces portgroup 2/0/0
Portgroup2/0/0 is up, line protocol is up
Received Frames:1472937898
Transmit Frames:1472937897
Giant/Runt Frame count:0
Code violation and running disparity error count(cvrd):30311179128
Number of times SF threshold exceeded:0
CDL HEC error count:0
SII Mismatch error count:0
Hardware is gefc_portgroup

```

About Latency and Transmit Buffers

The 8-port FC/GE aggregation card adds latency to the transmission of FC, FICON, and ISC traffic depending on the services configured. [Table 5-1](#) shows the various configurations on the transmitting node and the FC, FICON, and ISC latency values, both the time in microseconds and the equivalent distance in kilometers (in parentheses).



Note

The latency values shown in [Table 5-1](#) are only valid if flow control is disabled and inactive.

Table 5-1 FC, FICON, and ISC Latency Values for 8-Port FC/GE Aggregation Cards

Traffic Mix on Transmitting Node	Maximum Added End-to-End Latency ¹ (Time and Distance)			
	No GE	1518-Byte GE Packets	4470-Byte GE Packets	10,232-Byte GE Packets
FC/FICON/ISC only on the 2.5-Gbps aggregated signal carried over a 2.5-Gbps ITU trunk card	18.8 microseconds (3.8 km)			
FC/FICON/ISC only on a 2.5-Gbps aggregated signal carried over a 10-Gbps ITU trunk card	19.9 microseconds (4.0 km)			
FC/FICON/ISC only on a 2.5-Gbps aggregated signal mixed with GE on the same 10-Gbps ITU trunk card		22.2 microseconds (4.4 km)	24.8 microseconds (5.0 km)	36.3 microseconds (7.3 km)

Table 5-1 FC, FICON, and ISC Latency Values for 8-Port FC/GE Aggregation Cards (continued)

FC/FICON/ISC and GE on the same 2.5-Gbps aggregated signal carried over a 2.5-Gbps ITU trunk card		27.9 microseconds (5.6 km)	47.1 microseconds (9.4 km)	83.6 microseconds (16.7 km)
FC/FICON/ISC and GE on the same 2.5-Gbps aggregated signal carried over a 10-Gbps ITU trunk card		39.2 microseconds (7.8 km)	77.1 microseconds (15.4 km)	151.1 microseconds (30.2 km)

1. The latency values are based on configuration of correct transmit buffer sizes as described in [Table 5-2](#).

The transmit buffer on the receiving node compensates for the packet jitter effects due to service multiplexing on the trunk. You must correctly configure the size of this transmit buffer to ensure that no buffer underflow or overflow occurs. Symptoms of an improperly configured transmit buffer on the gigabitphy interface include CRC errors, frame drops, and transmission word errors detected by the receiving FC, FICON, or ISC client node.

**Note**

We strongly recommend configuring port pairs as FC/FICON/ISC only or GE only. Mixing FC, FICON, or ISC and GE in a port pair increases the FC, FICON, or ISC signal latency between the nodes.

Configuring Transmit Buffer Size for FC, FICON, and ISC

To configure the transmit buffer on the receiving node, perform the following steps, starting in global configuration mode:


	Command	Purpose
Step 1	Switch(config)# interface gigabitphy slot/0/port Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# shutdown	Disables the interface.
Step 3	Switch(config-if)# tx-buffer size bytes	Configures the transmit buffer size. The default value is 256 bytes. The range is 256 to 13824.
		 <p>Caution Issuing the tx-buffer size command might momentarily disrupt traffic through the interface.</p>
Step 4	Switch(config-if)# no shutdown	Enables the interface.

Table 5-2 provides transmit buffer settings for various configurations possible on the remote node.

Table 5-2 FC, FICON, and ISC Transmit Buffer Settings

Traffic Mix on the Transmitting Node	Transmit Buffer Size (in Bytes) on the Receiving Node			
	No GE	1518-Byte GE Packets	4470-Byte GE Packets	10,232-Byte GE Packets
FC/FICON/ISC only on the 2.5-Gbps aggregated signal carried over a 2.5-Gbps ITU trunk card	256 (default)			
FC/FICON/ISC only on a 2.5-Gbps aggregated signal carried over a 10-Gbps ITU trunk card	256 (default)			
FC/FICON/ISC only on a 2.5-Gbps aggregated signal mixed with GE on the same 10-Gbps ITU trunk card		384	640	1280
FC/FICON/ISC and GE on the same 2.5-Gbps aggregated signal carried over a 2.5-Gbps ITU trunk card		768	1792	3712
FC/FICON/ISC and GE on the same 2.5Gbps aggregated signal carried over a 10-Gbps ITU trunk card		1280	3584	7296



Note

The transmit buffer must be configured correctly for all gigabitphy interfaces encapsulated for FC, FICON, or ISC traffic regardless of the flow control mode configured on the interfaces.

Example

The following example shows how to configure the transmit buffer size on the receiving node:

```
Switch(config)# interface gigabitphy 2/0/0
Switch(config-if)# shutdown
Switch(config-if)# tx-buffer size 1280
Switch(config-if)# no shutdown
```

Displaying Transmit Buffer Configuration

To display the transmit buffer configuration, use the following EXEC command:

Command	Purpose
<code>show interfaces gigabitphy slot/0/slot</code>	Displays the interface configuration.

Example

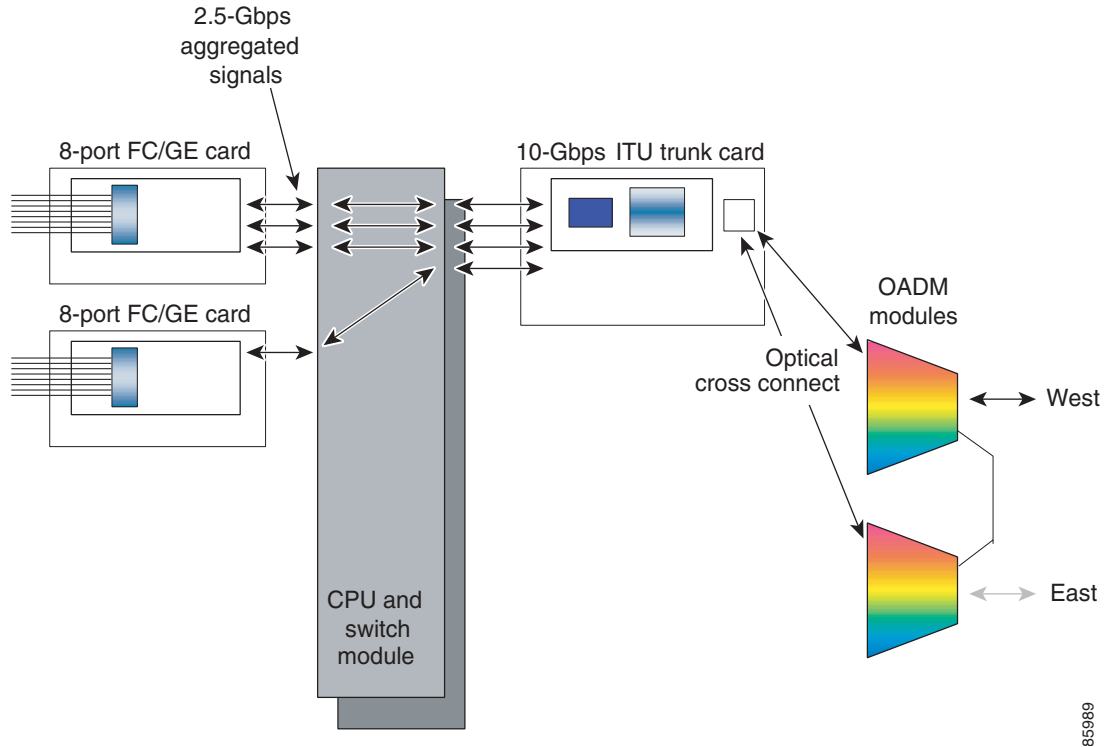
The following example shows how to display the transmit buffer configuration:

```
Switch# show interfaces gigabitphy 2/0/0
GigabitPhy2/0/0 is up, line protocol is up
  Optical Transceiver: Multi-Mode
  Signal quality: Good
  Encapsulation: GigabitEthernet
  Time of last "encapsulation" change 3d18h
  Forward laser control: Off
  Flow-identifier: 20
  Loopback not set
  Threshold monitored for: None
  Received Frames: 0
  Received Bytes: 0
  Transmit Frames: 0
  Transmit Bytes: 0
  Code violation and running disparity error count( 8b10b cvrd): 760759
  RX CRC errors: 0
  TX CRC errors: 0
  Giant Packets: 0
  Runt Packets: 0
  5 minute input rate 0 bits/sec, 0 frames/sec
  5 minute output rate 0 bits/sec, 0 frames/sec
  Transmit Buffer size is 256 bytes
  MTU size is 10232 bytes
  Hardware is gige_fc_phy_port
```

About Cross Connections

The client signal follows a path of interface optical cross connections through the Cisco ONS 15530. [Figure 5-1](#) shows an example of cross connections. Knowing the path of a signal through the shelf helps with system management and troubleshooting.

Figure 5-1 Optical Cross Connection Example



65989

Configuring Cross Connections

The aggregated signals from the 8-port FC/GE aggregation cards pass through the switch fabric to the 2.5-Gbps ITU trunk card, 10-Gbps ITU trunk card, or the 10-Gbps uplink card. To establish a cross connection through the switch fabric, perform the following steps, beginning in global configuration mode:

Command	Purpose
Switch(config)# connect <i>interface1</i> <i>interface2</i>	Creates a cross connection between two interfaces through the switch fabric.

Examples

The following example shows how to configure a cross connection between an 8-port FC/GE aggregation card and a 2.5-Gbps ITU trunk card:

```
Switch(config)# connect portgroup 2/0/0 waveethernetphy 3/0
```

The following example shows how to configure a cross connection between an 8-port FC/GE aggregation card and a 10-Gbps ITU trunk card:

```
Switch(config)# connect portgroup 2/0/0 waveethernetphy 3/0.1
```

The following example shows how to configure a cross connection between an 8-port FC/GE aggregation card and a 10-Gbps uplink card:

```
Switch(config)# connect portgroup 2/0/0 tengiethernetphy 3/0.1
```

Displaying the Cross Connection Configuration

To display the cross connection configuration, use the following privileged EXEC command:

Command	Purpose
show connect [edge intermediate [sort-channel interface <i>interface</i>]]	Displays the signal cross connection configuration through the system.

Examples

The following example shows the cross connections:

```
Switch# show connect
Index Client Intf      Trunk Intf      Kind      C2TStatus  T2CliStatus
-----
15     Port3/0/0      WaveE8/0.1     Provisioned Up          Up
```

The following example shows the intermediate cross connections:

```
Switch# show connect intermediate
client/      wave      wave      wdm
wave         client    patch     filter    trk      channel
-----
Giga2/0/0    TenGE7/0  Giga2/0/1  TenGE7/0
```

About Alarm Thresholds

You can configure thresholds on the 8-port FC/GE aggregation card interfaces that issue alarm messages to the system if the thresholds are exceeded.

Every second, the monitoring facility updates the counters that correspond to the alarm thresholds. When the signal degrades, or fails entirely, the system issues alarms to the console. These alarms can help isolate failures in the system and in the network.

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

Configuring Alarm Thresholds

To configure alarm thresholds on the 8-port FC/GE aggregation card interfaces, perform the following steps, beginning in global configuration mode:

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

	Command	Purpose
Step 3	Switch(config-t-list)# threshold name {cvrd cdl hec crc sonet-sdh section cv tx-crc} {failure degrade} [index value] Switch(config-threshold)#	Specifies a threshold type to modify and enters threshold configuration mode.
Step 4	Switch(config-threshold)# value rate value	Specifies the threshold rate value. This value is the negative power of 10 (10 ⁻ⁿ).
Step 5	Switch(config-threshold)# description text	Specifies a description of the threshold. The default value is the null string. (Optional)
Step 6	Switch(config-threshold)# exit Switch(config-t-list)#	Returns to threshold list configuration mode. Repeat Step 3 through Step 6 to configure more thresholds in the threshold list.
Step 7	Switch(config-t-list)# exit Switch(config)#	Returns to global configuration mode.
Step 8	Switch(config)# interface interface Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 9	Switch(config-if)# threshold-group name	Configures the threshold list on the interface.

Table 5-3 lists the threshold error rates in errors per second for 8-port FC/GE signals.

Table 5-3 Threshold Values for Monitored Rates for FC/FICON/GE Signals in Errors Per Second

Rate	FC/FICON/GE CRC ¹	FC/FICON/GE CVRD ²
3	83333	1244390
4	58235	124944
5	9423	12499
6	994	1250
7	100	125
8	100	12
9	10	1

1. CRC=cyclic redundancy check

2. CVRD= code violation and running disparity error



Note

Portgroup interfaces have a default alarm threshold list that raises signal failure alarms for CVRD errors. The default rate value is 5.

Example

The following example shows how to create an alarm threshold list and configure that list for 8-port FC/GE aggregation card interfaces:

```
Switch# configure terminal
Switch(config)# threshold-list gigabitphy-counters
Switch(config-t-list)# threshold name tx-crc degrade
Switch(config-threshold)# value rate 9
```

```
Switch(config-threshold)# exit
Switch(config-t-list)# threshold name tx-crc failure
Switch(config-threshold)# value rate 7
Switch(config-threshold)# exit
Switch(config-t-list)# exit
Switch(config)# interface gigabitphy 3/0/0
Switch(config-if)# threshold-group gigabitphy-counters
```

Displaying the Alarm Threshold Configuration

To display the configuration of a threshold list and the threshold group for an gigabitphy interface, use the following EXEC commands:

Command	Purpose
show threshold-list [<i>name</i>]	Displays the threshold group configuration.
show interfaces gigabitphy <i>slot/subcard/slot</i>	Displays the interface configuration.

Examples

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

```
Switch# show threshold-list gigabitphy-counters
```

```
Threshold List Name: gigabitphy-counters
Notification throttle timer : 5 (in secs)
Threshold name : CRC Severity : Degrade
Value : 10e-9
APS Trigger : Not set
Threshold name : CRC Severity : Failure
Value : 10e-7
APS Trigger : Not set
```

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

```
Switch# show interfaces gigabitphy 3/0/0
GigabitPhy3/0/0 is up, line protocol is up
Signal quality: Good
Forward laser control: Off
Configured threshold Group: gigabitphy-counters
Threshold monitored for: CRC
SF set value: 10e-7 (20 in 1 secs)
SD set value: 10e-9 (1 in 5 secs)
Received Frames: 0
Transmit Frames: 0
Code violation and running disparity error count(cvrd): 0
Number of times SF threshold exceeded: 0
Number of times SD threshold exceeded: 0
CRC error count: 0
Number of times SF threshold exceeded: 0
Number of times SD threshold exceeded: 0
Egress Packet Sequence error count: 0
Egress Packet Indicated error count: 0
5 minute input rate 0 bits/sec, 0 frames/sec
5 minute output rate 0 bits/sec, 0 frames/sec
Hardware is escon_phy_port
```




Configuring Transponder Line Card Interfaces

This chapter describes how to configure interfaces and patch connections on the Cisco ONS 15530. This chapter includes the following sections:

- [Configuring Protocol Encapsulation or Clock Rate, page 6-2](#)
- [About Transponder Line Card Channel Frequencies, page 6-6](#)
- [Configuring Transponder Line Card Channel Frequency, page 6-6](#)
- [About Protocol Monitoring, page 6-7](#)
- [Configuring Protocol Monitoring, page 6-9](#)
- [About Alarm Thresholds, page 6-10](#)
- [Configuring Alarm Thresholds, page 6-11](#)
- [About Laser Shutdown, page 6-14](#)
- [Configuring Laser Shutdown, page 6-17](#)
- [Configuring Optical Power Thresholds, page 6-19](#)
- [About Patch Connections, page 6-21](#)
- [Configuring Patch Connections, page 6-21](#)
- [About Cross Connections, page 6-23](#)



Note

To ensure the installed Cisco IOS software supports your hardware and provides the software features you wish to use, see the [“New and Changed Information” section on page xiii](#). Also refer to the [“Hardware Supported”](#) section and [“Feature Set”](#) section of the latest release notes for the Cisco ONS 15530.

To configure transparent interfaces on the Cisco ONS 15530, 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** Specify the laser frequency (optional).
 - Step 3** Enable protocol monitoring (optional).
 - Step 4** Create alarm threshold lists and apply them to the interfaces (optional).
 - Step 5** Enable forward laser control (optional).
-

To configure wave interfaces on the Cisco ONS 15530, 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 15530, perform the following steps:

-
- Step 1** Configure the patch connections between the OADM modules and the wavepatch interface of the transponder line card (required).
 - Step 2** Configure the patch connections between the OSC (optical supervisory channel) interface on the OADM modules and the wavepatch interface of the OSC (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 }	Specifies Fast Ethernet, FDDI, Gigabit Ethernet, or ESCON. OFC ¹ is disabled.
	Switch(config-if)# encapsulation sysplex clo	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	Specifies Sysplex ETR ³ . OFC is disabled.
	Switch(config-if)# encapsulation sysplex isc { compatibility peer [1g 2g] }	Specifies ISC ⁴ links compatibility mode (1 Gbps) or peer mode (1 Gbps or 2 Gbps). OFC is enabled for compatibility mode and disabled for peer mode. The default rate for peer mode is 2 Gbps.
	Switch(config-if)# encapsulation ficon { 1g 2g }	Specifies FICON encapsulation and rate. OFC is disabled.
	Switch(config-if)# encapsulation sonet { oc3 oc12 oc48 }	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 }	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 }]	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 6-14.
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 15530 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.

**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 6-7](#).

**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 10, “Configuring APS.”](#)

**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 15530 because of the nature of the traffic type.

[Table 6-1](#) lists the clock rates for well-known protocols supported by the transponder line card:

Table 6-1 Supported Clock Rates for Well-Known Protocols

Well-Known Protocol	Clock Rate (in kbps)	Well-Known Protocol	Clock Rate (in kbps)
DS3	44,736	Gigabit Ethernet	1,250,000
DV1 ¹ in ADI ² mode	270,000	ISC Compatibility Mode (ISC-1)	1,062,500
E3	34,368	ISC Peer Mode (ISC-3)	2,125,000
ESCON	200,000	SONET OC-1	51,840
Fibre Channel (1 Gbps)	1,062,500	SONET OC-3/SDH STM-1	155,520
Fibre Channel (2 Gbps)	2,125,000	SONET OC-12/SDH STM-4	622,080
FICON (1 Gbps)	1,062,500	SONET OC-24	1,244,160
FICON (2 Gbps)	2,125,000	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 15530 transponder line cards. 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.

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 10/0/0
Transparent10/0/0 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 Transponder Line Card Channel Frequencies

The transponder line card supported by the Cisco ONS 15530 is tunable to one of two frequencies. These frequencies are adjacent on the ITU grid. For example, a transponder line card can support the frequencies for channel 5 and channel 6, but not for channel 5 and channel 8. By default, the transponder line card operates at the laser frequency for the lower channel number. However, you can configure the transponder line card to operate at the laser frequency for the higher channel number using the CLI.

Configuring Transponder Line Card Channel Frequency

To select the desired channel frequency for the transponder line cards supported by the Cisco ONS 15530, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface wave <i>slot/subcard</i>	Selects the wave interface to configure and enters interface configuration mode.
	Switch(config-if)#	
Step 2	Switch(config-if)# laser frequency <i>number</i>	Selects one of the two frequencies in GHz supported by the laser. The default is the lower frequency for the transponder module.



Note

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

Example

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

```
Switch(config)# interface wave 10/0
Switch(config-if)# laser frequency 195700
```

Displaying Transponder Line Card Channel Frequency

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

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

Example

The following example shows how to display the transponder line card channel frequency:

```
Switch# show interface wave 10/0
Wave10/0 is down, line protocol is down
Channel: 30   Frequency: 195.7 Thz   Wavelength: 1531.90 nm
Active Wavepatch : Wavepatch10/0/0
Splitter Protected: No
Signal quality: Loss of light
Receiver power level:
```

```
Forward laser control: Off
Laser safety control: Off
Osc physical port: No
Wavelength used for inband management: No
Configured threshold Group: None
Loopback not set
Last clearing of "show interface" counters never
Hardware is data_only_port
```

About Protocol Monitoring

Transparent interfaces on the Cisco ONS 15530 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)
- FC (Fibre Channel) (1 Gbps and 2 Gbps)
- FICON (Fiber Connection) (1 Gbps and 2 Gbps)
- GE (Gigabit Ethernet)
- ISC (InterSystem Channel) links peer mode
- ISC links compatibility 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 line card functional image to release 1.A3.

For GE, FC, and FICON traffic, the Cisco ONS 15530 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 15530 monitors the SONET section overhead only, not the SONET line overhead. Specifically, the Cisco ONS 15530 monitors the B1 byte and the framing bytes. The system can detect the following defect conditions:

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

- Severely errored frame
- Loss of frame

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

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

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

For ISC links compatibility and peer mode traffic, the system monitors the following conditions:

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

Configuring Protocol Monitoring

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

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

Examples

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

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

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

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

Displaying Protocol Monitoring Configuration

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

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

Examples

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

```
Switch# show interfaces transparent 10/0/0
Transparent10/0/0 is up, line protocol is up
  Encapsulation: Sonet   Rate: oc3
→  Signal monitoring: on
  Forward laser control: Off
  Configured threshold Group: None
→  Section code violation error count(bipl): 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 7/0
Wave7/0 is up, line protocol is up
  Channel: 31   Frequency: 195.8 Thz   Wavelength: 1531.12 nm
  Active Wavepatch : Wavepatch7/0/0
  Splitter Protected: No
  Signal quality: Good
  Receiver power level: -14.71 dBm
  Forward laser control: Off
  Laser safety control: Off
  Osc physical port: No
  Wavelength used for inband management: No
  Configured threshold Group: None
  Loopback not set
  Last clearing of "show interface" counters 09:20:01
  Hardware is data_only_port
```

About Alarm Thresholds

You can configure thresholds on transparent and wave interfaces that issue alarm messages to the system if the thresholds are exceeded. The threshold values are applied to both transparent and wave interfaces on a transponder line card 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 it is reserved for use by the system.

Configuring Alarm Thresholds

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

	Command	Purpose
Step 1	Switch(config)# threshold-list <i>name</i> Switch(config-t-list)#	Creates or selects the threshold list to configure and enters threshold list configuration mode. Note You cannot modify an existing threshold list if it is associated with an interface.
Step 2	Switch(config-t-list)# notification-throttle timer <i>seconds</i>	Configures the SNMP notification timer. The default value is 5 seconds. (Optional)
Step 3	Switch(config-t-list)# threshold name { cvrd cdl hec crc sonet-sdh section cv tx-crc } { failure degrade } [<i>index value</i>] Switch(config-threshold)#	Specifies a threshold type to modify and enters threshold configuration mode.
Step 4	Switch(config-threshold)# value rate <i>value</i>	Specifies the threshold rate value. This value is the negative power of 10 (10 ⁻ⁿ).
Step 5	Switch(config-threshold)# description <i>text</i>	Specifies a description of the threshold. The default value is the null string. (Optional)
Step 6	Switch(config-threshold)# aps trigger	Enables APS switchover when this threshold is crossed. (Optional) Note This command only triggers switchovers for y-cable protection, not for splitter protection.
Step 7	Switch(config-threshold)# exit Switch(config-t-list)#	Returns to threshold list configuration mode. Repeat Step 3 through Step 7 to configure more thresholds in the threshold list.
Step 8	Switch(config-t-list)# exit Switch(config)#	Returns to global configuration mode.
Step 9	Switch(config)# interface { transparent slot/subcard/0 wave slot/subcard } Switch(config-if)#	Selects the transparent or wave interface to configure and enters interface configuration mode.
Step 10	Switch(config-if)# threshold-group <i>name</i>	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.

Table 6-2 lists the threshold error rates in errors per second for each of the protocol encapsulations.

Table 6-2 Thresholds for Monitored Protocols in Errors Per Second

Rate	SONET OC-3 or SDH STM-1	SONET OC-12 or SDH STM-4	SONET OC-48 or SDH STM-16	Gigabit Ethernet	ESCON	FICON ¹	Fibre Channel ²	ISC ³
3	31,753	32,000	32,000	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. One Gbps rate only.
3. 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 5/0/0
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)# encapsulation 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)# encapsulation sonet oc3
Switch(config-if)# monitor enable
Switch(config-if)# threshold-group sonet-alarms
```

Displaying Alarm Threshold Configuration

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

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

Examples

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

```
Switch# show threshold-list sonet-counters

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

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

```
Switch# show interfaces transparent 3/0/0
Transparent3/0/0 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 15530 supports mechanisms to automatically shut down transponder line card lasers. The three types of laser shutdown mechanisms are:

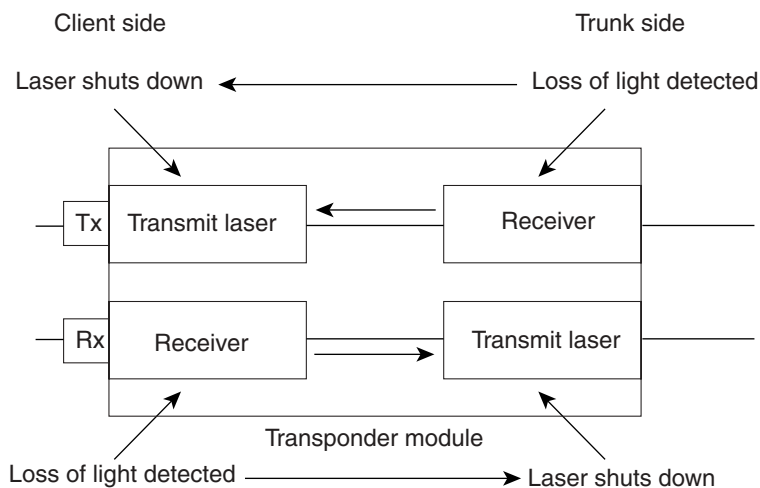
- Forward laser control
- OFC safety protocol
- Laser safety control

About Forward Laser Control

When loss of light occurs on the receive signal of a transparent or wave interface, the corresponding transmitting laser on the other side of the transponder line card continues to function and might send unreliable information to the client. Forward laser control provides a means to quickly shut down a transmitting laser when such a receive signal failure occurs (see [Figure 6-1](#)). The receive signal loss of light can result from a failure in the client equipment, a receiver failure in the transponder line card, or a laser shutdown on another node in the network.

This feature is convenient for configurations, such as Sysplex, where signal protection is performed in the client hardware and a quick laser shutdown causes a quick path switchover.

Figure 6-1 Forward Laser Control Overview

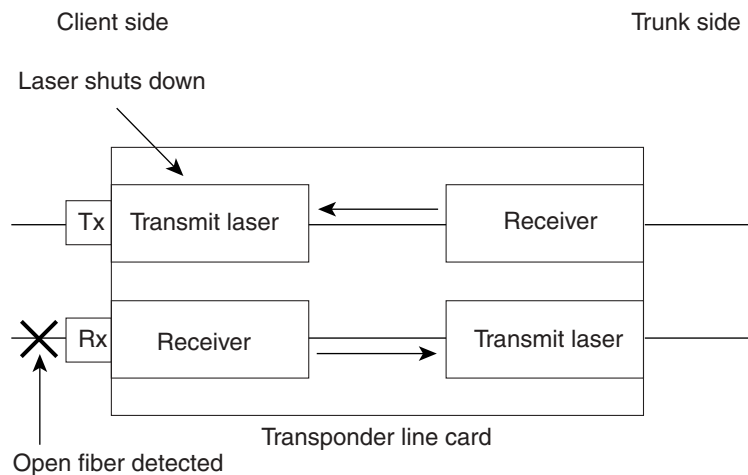


58863

About OFC

The Cisco ONS 15530 allows you to enable the OFC safety protocol on the client side interfaces. When the system detects an “open fiber,” the laser that transmits to the client equipment shuts down. An open fiber condition occurs when the connectors to the client equipment are detached from the transponder line card ports or when the fiber is cut (see [Figure 6-2](#)).

Figure 6-2 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 15530 interoperates with OFC-standard-compliant client equipment.



Caution

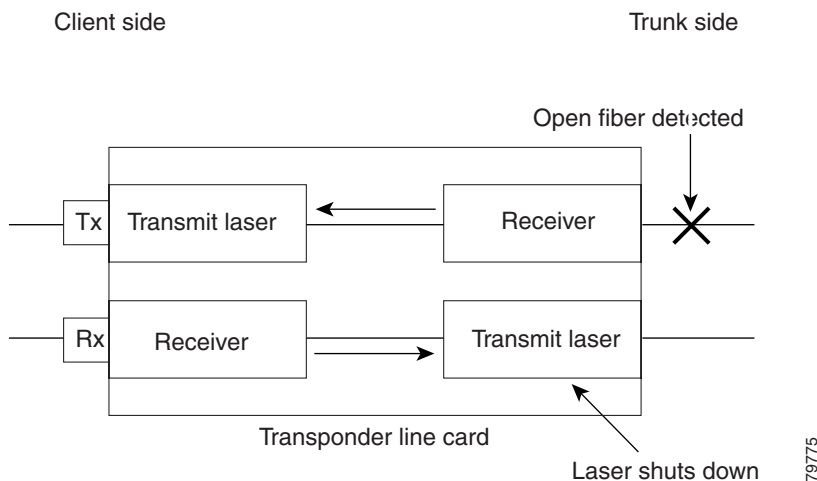
Do not configure OFC with either forward laser control or laser safety control. Combining these features interferes with the OFC protocol.

Use the **encapsulation** command, described in the “[Configuring Transponder Line Card Channel Frequency](#)” section on [page 6-6](#) to configure OFC on a transparent interface.

About Laser Safety Control

The Cisco ONS 15530 allows you to enable laser safety control on the trunk side interfaces of the transponder line cards and the 2.5-Gbps ITU trunk cards. Much like OFC, the laser safety control protocol shuts down the transponder line card laser transmitting to the trunk when a fiber cut occurs or when the trunk fiber is detached from the shelf (see [Figure 6-3](#)).

Figure 6-3 Laser Safety Control Overview



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

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



Caution

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

Configuring Laser Shutdown

This sections describes how to configure forward laser control and laser safety control on the Cisco ONS 15530 transponder line card interfaces.



Note

To function correctly, configure forward laser control on both the transparent and wave interfaces on a transponder line card. For y-cable protection, forward laser control on both the transparent and wave interfaces on both transponder line cards will be configured automatically.

Configuring Forward Laser Control

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

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



Caution

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

Examples

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

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

Displaying Forward Laser Control Configuration

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

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

Example

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

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

Configuring Laser Safety Control

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

	Command	Purpose
Step 1	Switch(config)# interface wave <i>slot/subcard</i> 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
<code>show interfaces wave <i>slot/subcard</i></code>	Displays interface information.

Example

The following example shows how to display the laser safety control configuration for an 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: 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 line card, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface wavepatch <i>slot/subcard/port</i> Switch(config-if)#	Selects the transparent interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# optical threshold power receive {low high} {alarm warning} value [severity {critical major minor not alarmed not reported}]	Specifies the optical power threshold value in units of 0.1 dBm. The default values for the active wavepatch interfaces 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 The default values for the standby wavepatch interfaces are as follows: Low alarm: -28 dBm Low warning: -24 dBm High warning: -15 dBm High alarm: -13 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 line card:

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

Displaying Optical Power Threshold Configuration

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

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

Example

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

```
Switch# show interfaces wavepatch 4/0/0
Wavepatch4/0/0 is up, line protocol is up
Receiver power level: -23.91 dBm
Optical threshold monitored for : Receive Power (in dBm)
Low alarm value = -28.0 (default)
```

```

Low Alarm Severity = major
Low warning value = -24.0 (default)
Low Warning Severity = not alarmed
High alarm value = -8.0 (default)
High Alarm Severity = major
High warning value = -10.0 (default)
High Warning Severity = not alarmed
Hardware is passive_port

```

About Patch Connections

Because the OADM modules are passive devices, the Cisco ONS 15530 does not detect its optical patch connection configuration. For system management purposes, you must also configure the patch connection configuration using the CLI.

Table 6-3 describes the types of patch connections on the Cisco ONS 15530.

Table 6-3 Patch Connection Types

Patch Connection	Description
Thru interface to thru interface	Connection between two OADM modules in different chassis slots.
Wavepatch interface to filter interface or filter interface to wavepatch interface	Connection between the wavepatch on a transponder line card and the filter interface on an OADM module.
OSC wave interface to oscfilter interface or oscfilter interface to OSC wave interface	Connection between the OSC wave interface and the oscfilter interface on the OADM module in the same chassis slot.

For more information on patch connection rules, refer to the *Cisco ONS 15530 Planning and Design Guide*.

Configuring Patch Connections

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

Command	Purpose
patch thru <i>slot1/subcard1</i> thru <i>slot2/subcard2</i>	Configures the patch connection between two add/drop OADM modules in different chassis slots.
patch wavepatch <i>slot1/subcard1/port1</i> filter <i>slot2/subcard2/port2</i> or patch filter <i>slot1/subcard1/port1</i> wavepatch <i>slot2/subcard2/port2</i>	Configures the patch connection between a transponder line card and a OADM module.
patch wave <i>slot/subcard</i> oscfilter <i>slot/subcard</i> or patch oscfilter <i>slot/subcard</i> wave <i>slot/subcard</i>	Connection between the OSC wave interface and the oscfilter interface on the OADM module in the same chassis slot.

**Note**

If you correctly patch your OADM 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 12-3](#).

Example

The following example shows how to configure the patch connections:

```
Switch# configure terminal
Switch(config)# patch thru 0/0 thru 0/1
Switch(config)# patch wave 1/0 oscfilter 0/0
Switch(config)# patch wave 1/1 oscfilter 0/1
Switch(config)# patch wavepatch 4/0/0 filter 0/0/1
Switch(config)# patch wavepatch 4/0/1 filter 0/1/1
```

Displaying Patch Connections

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

Command	Purpose
show patch [detail]	Displays the patch connections.

**Note**

The error field in the **show patch** command output helps troubleshoot shelf misconfigurations. When there is a channel mismatch between a transponder line card and a OADM module, “Channel Mismatch” appears for the patch connection. When more than one OADM 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 15530. Knowing the path of a signal through the shelf helps with system management and troubleshooting.

Displaying Cross Connections

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

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

Examples

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

```
Switch# show connect intermediate
client/      wave      wave      wdm
wave        client    patch    filter  trk  channel
-----
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
```




Configuring Trunk and Uplink Card Interfaces

This chapter describes how to configure 2.5-Gbps ITU trunk cards, 10-Gbps ITU trunk cards, and 10-Gbps uplink cards on the Cisco ONS 15530. This chapter includes the following sections:

- [Configuring 2.5-Gbps ITU Trunk Card Interfaces, page 7-1](#)
- [Configuring 10-Gbps ITU Trunk Card Interfaces, page 7-4](#)
- [Configuring 10-Gbps Uplink Card Interfaces, page 7-7](#)
- [About Cross Connections, page 7-9](#)
- [Configuring Cross Connections, page 7-10](#)
- [About Alarm Thresholds, page 7-11](#)
- [Configuring Alarm Thresholds, page 7-12](#)
- [About Patch Connections, page 7-15](#)
- [Configuring Patch Connections, page 7-15](#)



Note

To ensure the installed Cisco IOS software supports your hardware and provides the software features you wish to use, see the [“New and Changed Information” section on page xiii](#). Also refer to the [“Hardware Supported” section](#) and [“Feature Set” section](#) of the latest release notes for the Cisco ONS 15530.

Configuring 2.5-Gbps ITU Trunk Card Interfaces

To configure the 2.5-Gbps ITU trunk card interface, perform the following tasks, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface waveethernetphy slot/0 Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# laser frequency number	Selects one of the two frequencies in GHz supported by the laser. The default is the lower frequency for the 2.5-Gbps ITU trunk card. (Optional)
Step 3	Switch(config-if)# [no] loopback [facility terminal]	Enables or disables internal loopback for testing and defect isolation. (Optional)

	Command	Purpose
Step 4	Switch(config-if)# [no] laser control safety enable	Enables or disables laser safety control.
Step 5	Switch(config-if)# [no] laser shutdown	Turns the laser on and off. (Optional) Note The laser must warm up for 2 minutes before carrying traffic.
Step 6	Switch(config-if)# [no] cdl defect-indication force hop-endpoint	Enables or disables hop endpoint for in-band message channel defect indications when APS is not configured (Optional).
Step 7	Switch(config-if)# no shutdown	Enables the interface.
Step 8	Switch(config-if)# exit Switch(config)	Returns to global configuration mode.
Step 9	Switch(config)# interface wavepatch slot/0/0 Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 10	Switch(config-if)# optical threshold power receive {low high} {alarm warning} value [severity {critical major minor not alarmed not reported}]	Specifies the optical power receive threshold value in units of 0.1 dBm. The default values are as follows: Low alarm: -28 dBm Low warning: -26 dBm High warning: -10 dBm High alarm: -8 dBm Alarm severity: major Warning severity: not alarmed
Step 11	Switch(config-if)# [no] shutdown	Enables or disables the interface. Repeat Step 9 and Step 11 on wavepatch slot/0/1 for splitter 2.5-Gbps ITU trunk cards.

**Caution**

Loopbacks on waveethernetphy interfaces disrupt service. Use this feature with care.

**Note**

For configuration information for the ethernetdcc interface, see the “[Configuring IP on Ethernetdcc Interfaces for the In-Band Message Channel](#)” section on page 12-12.

Example

The following example shows how to configure 2.5-Gbps ITU trunk card waveethernetphy interfaces:

```
Switch(config)# interface waveethernetphy 10/0
Switch(config-if)# cdl defect-indication force hop-endpoint
Switch(config-if)# no shutdown
```


Displaying the 2.5-Gbps ITU Trunk Card Interface Configuration

To display the configuration of 2.5-Gbps ITU trunk card interfaces, use the following EXEC command:

Command	Purpose
show interfaces { waveethernetphy slot/0 wavepatch slot/0/port }	Displays the interface configuration.

Examples

The following example shows how to display the configuration of a waveethernetphy interface:

```
Switch# show interfaces waveethernetphy 1/0
WaveEthernetPhy1/0 is up, line protocol is up
 Channel: 1   Frequency: 192.1 Thz   Wavelength: 1560.61 nm
 Active Wavepatch      : Wavepatch1/0/0
 Splitter Protected    : No
 Signal quality        : Good
 Receive power level   : -6.45 dBm
 Laser shut down       : No
 Osc physical port     : No
 Wavelength used for inband management: No
 Loopback not set

Configured threshold Group: None
CDL HEC error count: 0
CRC error count: 0
Code violation and running disparity error count( 64b66b cvrd): 0

Defect Indication Status      : up
Configured Node Behavior      : Hop Terminating
Current Node Behavior         : Hop Terminating
Defect Indication Receive     : FDI-H FDI-E
Defect Indication Transmit    : BDI-H

Tx Frames sent to N/W         : 218707020912

Tx Frames rcvd from Client    : 0
Tx CRC Errors                 : 0
Tx HEC Errors                 : 0
Tx QuadPHY sybl Errs         : 4257380395
Tx Dropped Frames             : 0
Tx Oversize Frames            : 0
Tx Undersize Frames           : 0
Tx Idle Frames from Fabric    : 0
Tx Generated CDL Idle Frames  : 218720041509
(having an SII of 255)

Rx Frames rcvd from N/W       : 218719304600

Rx Frames sent to Client      : 647
Rx CRC Errors                 : 0
Rx HEC Errors                 : 0
Rx MII (Decoder) Errors       : 0
Rx Dropped Frames             : 0
Rx Oversize Frames            : 0
Rx Undersize Frames           : 0
Rx Total Drpd Idle Frames     : 218719303953
Rx Dropped CDL Idle Frames    : 218719301229
(having an SII of 255)

Last clearing of "show interface" counters never
```

```

Hardware is data_enabled_port
Switch#sh int wavepatch 1/0/0
Wavepatch1/0/0 is up, line protocol is up
Receiver power level: -6.46 dBm

Optical threshold monitored for : Receive Power (in dBm)
Threshold exceeded for : High Warning and High Alarm
Low alarm value           = -28.0 (default)
Low Alarm Severity        = major
Low warning value         = -26.0 (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

```

The following example shows how to display the configuration of a wavepatch interface:

```

Switch# show interfaces wavepatch 1/0/0
Wavepatch1/0/0 is up, line protocol is up
Receiver power level: -6.46 dBm

Optical threshold monitored for : Receive Power (in dBm)
Threshold exceeded for : High Warning and High Alarm
Low alarm value           = -28.0 (default)
Low Alarm Severity        = major
Low warning value         = -26.0 (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

```

Configuring 10-Gbps ITU Trunk Card Interfaces

To configure the 10-Gbps ITU trunk card interface, perform the following tasks, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface waveethernetphy slot/0 Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# [no] loopback [facility terminal]	Enables or disables internal loopback for testing and defect isolation. (Optional)
Step 3	Switch(config-if)# [no] laser shutdown	Turns the laser on and off. (Optional) Note The laser must warm up for 2 minutes before carrying traffic.
Step 4	Switch(config-if)# [no] cdl defect-indication force hop-endpoint	Enables or disables hop endpoint for in-band message channel defect indications when APS is not configured. (Optional)
Step 5	Switch(config-if)# no shutdown	Enables the interface.

	Command	Purpose
Step 6	Switch(config-if)# exit Switch(config)	Returns to global configuration mode.
Step 7	Switch(config)# interface wavepatch slot/0/0 Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 8	Switch(config-if)# optical threshold power receive {low high} {alarm warning} value [severity {critical major minor not alarmed not reported}]	Specifies the optical power receive threshold value in units of 0.1 dBm. The default values are as follows: Low alarm: -22 dBm Low warning: -20 dBm High warning: -10 dBm High alarm: -8 dBm Alarm severity: major Warning severity: not alarmed
Step 9	Switch(config-if)# [no] shutdown	Enables or disables the interface. Repeat Step 7 and Step 9 on wavepatch slot/0/1 for splitter 10-Gbps ITU trunk cards.

**Caution**

Loopbacks on waveethernetphy interfaces disrupt service. Use this feature with care.

**Note**

For configuration information for the ethernetdcc interface, see the [“Configuring IP on Ethernetdcc Interfaces for the In-Band Message Channel”](#) section on page 12-12.

Example

The following example shows how to configure 10-Gbps ITU trunk card waveethernetphy interfaces:

```
Switch(config)# interface waveethernetphy 10/0
Switch(config-if)# cdl defect-indication force hop-endpoint
Switch(config-if)# no shutdown
```

Displaying the 10-Gbps ITU Trunk Card Interface Configuration

To display the configuration of 10-Gbps ITU trunk card interfaces, use the following EXEC command:

Command	Purpose
show interfaces { waveethernetphy slot/0[.subinterface] wavepatch slot/0/port }	Displays the interface configuration.

Examples

The following example shows how to display the configuration of a waveethernetphy interface:

```
Switch# show interfaces waveethernetphy 10/0
WaveEthernetPhy10/0 is down, line protocol is down
  Channel:30   Frequency:195.7 Thz   Wavelength:1531.90 nm
  Active Wavepatch      :Wavepatch10/0/1
  Splitter Protected    :No
  Signal quality        :Loss of lock
  Receive power level   : -35.0 dBm
  Laser Bias Current    :91 mA
  Laser Temperature     :31.0 degree C
  Laser shut down       :No
  Osc physical port     :No
  Wavelength used for inband management:No
  Loopback not set

  Configured threshold Group:None
  CDL HEC error count:0
  Number of times SF threshold exceeded:0
  Number of times SD threshold exceeded:0
  CRC error count:0
  Number of times SF threshold exceeded:0
  Number of times SD threshold exceeded:0
  Code violation and running disparity error count( 64b66b cvrd):0
  Number of times SF threshold exceeded:0
  Number of times SD threshold exceeded:0

  Defect Indication Status      :up
  Configured Node Behavior      :None
  Current Node Behavior         :Path Terminating
  Defect Indication Receive     :          None
  Defect Indication Transmit    :BDI-H

  Total Tx Frames Sent to N/W:  0
  Tx Gen CDL Idle Frame:        1843017892

  Rx Frames rcvd from N/W:      0
  Rx CRC Errors:                 0
  Rx HEC Errors:                 0
  Rx XGMII Errors:              0
  Rx IPG drpd pkts:             0
  Rx Idle Packets :              0
  Rx Oversize Frames :          0
  Rx Undersize Frames :         0

  Rx SII mismatch drpd data Frames :  0
  Rx SII mismatch drpd idle Frames :  0

  Last clearing of "show interface" counters never
  Hardware is data_enabled_port
```

The following example shows how to display the configuration of a waveethernetphy subinterface:

```
Switch# show interfaces waveethernetphy 10/0.1
WaveEthernetPhy10/0.1 is down, line protocol is down

Tx Frames Sent to N/W:          0
Tx HEC Errors:                  0
Tx CRC Errors:                  0
Tx QuadPHY sybl Errs:          55688870321
Tx Dropped Frames:              0
Tx Oversize Frames:             0
Tx Undersize Frames:            0
Tx Rcvd Idle Packets:           0

Rx Frames Sent to Clnt:         0
Rx FIFO full drpd pkts:        0
Rx Gen Idle pkt cnt:           0

Last clearing of "show interface" counters never
Hardware is data_enabled_port
```

The following example shows how to display the configuration of a wavepatch interface:

```
Switch# show interfaces wavepatch 3/0/0
Wavepatch3/0/0 is up, line protocol is up
Receiver power level:-9.86 dBm
Optical threshold monitored for :Receive Power (in dBm)
Threshold exceeded for :High Warning
Low alarm value = -22.0 (default)
Low Alarm Severity = major
Low warning value = -20.0 (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
```

Configuring 10-Gbps Uplink Card Interfaces

To configure the 10-Gbps uplink card interface, perform the following tasks, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface tengigethernetphy slot/0 Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# [no] loopback [facility terminal]	Enables or disables internal loopback for testing and defect isolation. (Optional)
Step 3	Switch(config-if)# [no] laser shutdown	Turns the laser on and off. (Optional)
Step 4	Switch(config-if)# [no] cdl defect-indication force hop-endpoint	Enables or disables hop endpoint for in-band message channel defect indications when APS is not configured. (Optional)
Step 5	Switch(config-if)# [no] shutdown	Enables or disables the interface.

**Caution**

Loopbacks on tengigethernetphy interfaces disrupt service. Use this feature with care.

**Note**

For configuration information for the ethernetccc interface, see the [“Configuring IP on Ethernetccc Interfaces for the In-Band Message Channel”](#) section on page 12-12.

Example

The following example shows how to configure 10-Gbps uplink card interfaces:

```
Switch(config)# interface tengigethernetphy 10/0
Switch(config-if)# cdl defect-indication force hop-endpoint
Switch(config-if)# no shutdown
```

Displaying the 10-Gbps Uplink Card Interface Configuration

To display the configuration of 10-Gbps uplink card interfaces, use the following EXEC command:

Command	Purpose
<code>show interfaces tengigethernetphy slot/0[.subinterface]</code>	Displays the interface configuration.

Example

The following example shows how to display the configuration of an tengigethernetphy interface:

```
Switch# show interfaces tengigethernetphy 3/0
TenGigEthernetPhy3/0 is up, line protocol is up
  Signal quality      :Good
  laser shut down    :Off
  Osc physical port   :No
  Loopback not set
  Wavelength used for inband management:No

  Configured threshold Group:None
  CDL HEC error count:0
  Number of times SF threshold exceeded:0
  Number of times SD threshold exceeded:0
  CRC error count:0
  Number of times SF threshold exceeded:0
  Number of times SD threshold exceeded:0
  Code violation and running disparity error count( 64b66b cvrd):0
  Number of times SF threshold exceeded:0
  Number of times SD threshold exceeded:0

  Defect Indication Status      :up
  Configured Node Behavior      :None
  Current Node Behavior         :Path Terminating
  Defect Indication Receive     :      None
  Defect Indication Transmit    :      None

  Total Tx Frames Sent to N/W:  48297
  Tx Gen CDL Idle Frame:       2173636535

  Rx Frames rcvd from N/W:      0
  Rx CRC Errors:                0
  Rx HEC Errors:                0
```

```
Rx XGMII Errors:          0
Rx IPG drpd pkts:        0
Rx Idle Packets :        1836560218
Rx Oversize Frames :     0
Rx Undersize Frames :    0

Rx SII mismatch drpd data Frames :    0
Rx SII mismatch drpd idle Frames :    1842816773

Last clearing of "show interface" counters never
Hardware is data_enabled_port
```

The following example shows how to display the configuration of a tengigethernetphy subinterface:

```
Switch# show interfaces tengigethernetphy 3/0.4
TenGigEthernetPhy3/0.4 is up, line protocol is up

Tx Frames Sent to N/W:      0
Tx HEC Errors:              0
Tx CRC Errors:              0
Tx QuadPHY sybl Errs:      37831687439
Tx Dropped Frames:         0
Tx Oversize Frames:         0
Tx Undersize Frames:        0
Tx Rcvd Idle Packets:      0

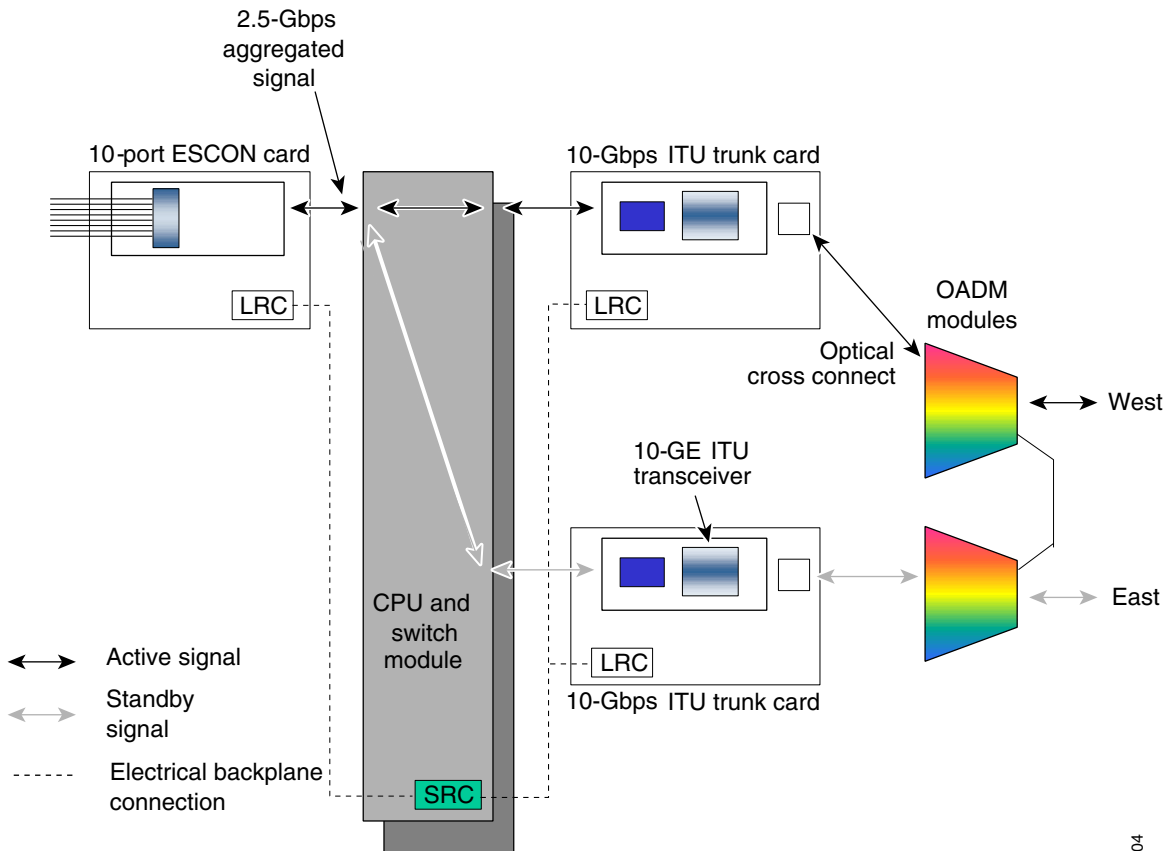
Rx Frames Sent to Clnt:     0
Rx FIFO full drpd pkts:    0
Rx Gen Idle pkt cnt:        0

Last clearing of "show interface" counters never
Hardware is data_enabled_port
```

About Cross Connections

The client signal follows a path of interface optical cross connections through the Cisco ONS 15530. [Figure 7-1](#) shows an example of cross connections. Knowing the path of a signal through the shelf helps with system management and troubleshooting.

Figure 7-1 Optical Cross Connection Example



79304

Configuring Cross Connections

The aggregated signal from the ESCON aggregation cards and the 8-port FC/GE aggregation cards passes through the switch fabric to the 2.5-Gbps ITU trunk card, 10-Gbps ITU trunk card, or the 10-Gbps uplink card. To establish a cross connection through the switch fabric, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# connect interface1 interface2	Creates a cross connection between two interfaces through the switch fabric.

Example

The following example shows how to configure a cross connection between an ESCON aggregation card and a 2.5-Gbps ITU trunk card:

```
Switch(config)# connect portgroup 2/0/0 waveethernetphy 3/0
```

The following example shows how to configure a cross connection between an ESCON aggregation card and a 10-Gbps ITU trunk card:

```
Switch(config)# connect portgroup 2/0/0 waveethernetphy 3/0.1
```


The following example shows how to configure a cross connection between an ESCON aggregation card and a 10-Gbps uplink card:

```
Switch(config)# connect portgroup 2/0/0 tengigetheretphy 3/0.1
```

Displaying the Cross Connection Configuration

To display the cross connection configuration, use the following privileged EXEC command:

Command	Purpose
show connect [edge intermediate] [sort-channel interface <i>interface</i>]	Displays the signal cross connection configuration through the system.

Examples

The following example shows the cross connections within a system for an ESCON signal:

```
Switch# show connect
Index Client Intf      Trunk Intf      Kind          C2TStatus  T2CliStatus
-----
15    Port3/0/0          WaveE8/0.1     Provisioned Up          Up
```

The following example shows the cross connections within a system for a transponder signal:

```
Switch# show connect intermediate
client/      wave          wave          wdm
wave        client        patch         filter        trk  channel
-----
Trans7/0/0  Wave7/0      7/0/0*       0/0/0         0/0   25
              7/0/1
```

About Alarm Thresholds

You can configure thresholds on the 2.5-Gbps ITU trunk card, 10-Gbps ITU trunk card, and 10-Gbps uplink interfaces that issue alarm messages to the system if the thresholds are exceeded.

Every second, the monitoring facility updates the counters that correspond to the alarm thresholds. When the signal degrades, or fails entirely, the system issues alarms to the console. These alarms can help isolate failures in the system and in the network.

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

Configuring Alarm Thresholds

To configure alarm thresholds on the 2.5-Gbps ITU trunk card, 10-Gbps ITU trunk card, and 10-Gbps uplink card interfaces, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# threshold-list <i>name</i> Switch(config-t-list)#	Creates or selects the threshold list to configure and enters threshold list configuration mode. Note You cannot modify an existing threshold list if it is associated with an interface.
Step 2	Switch(config-t-list)# notification-throttle timer <i>seconds</i>	Configures the SNMP notification timer. The default value is 5 seconds. (Optional)
Step 3	Switch(config-t-list)# threshold name { cvrd cdl hec crc sonet-sdh section cv tx-crc } { failure degrade } [index <i>value</i>] Switch(config-threshold)#	Specifies a threshold type to modify and enters threshold configuration mode.
Step 4	Switch(config-threshold)# value rate <i>value</i>	Specifies the threshold rate value. This value is the negative power of 10 (10 ⁻ⁿ).
Step 5	Switch(config-threshold)# description <i>text</i>	Specifies a description of the threshold. The default value is the null string. (Optional)
Step 6	Switch(config-threshold)# exit Switch(config-t-list)#	Returns to threshold list configuration mode. Repeat Step 3 through Step 6 to configure more thresholds in the threshold list.
Step 7	Switch(config-t-list)# exit Switch(config)#	Returns to global configuration mode.
Step 8	Switch(config)# interface <i>interface</i> Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 9	Switch(config-if)# threshold-group <i>name</i>	Configures the threshold list on the interface.

[Table 7-1](#) lists the threshold error rates in errors per second.

Table 7-1 Threshold Values for Monitored Rates in Errors Per Second

Rate	10-Gbps CVRD	10-Gbps CDL HEC	2.5-Gbps CVRD	2.5-Gbps CDL HEC
3	12,443,900	457901	19,968,416	1628
4	1,249,438	46765	2,055,776	166
5	124,944	4686	206,176	17
6	10,312	468	20,624	17
7	1031	47	2,064	17
8	103	4.7	208	17
9	10	0.47	24	17

Example

The following example shows how to create an alarm threshold list and configure that list for 10-Gbps ITU trunk card interfaces:

```
Switch# configure terminal
Switch(config)# threshold-list cvrd-counters
Switch(config-t-list)# threshold name cvrd degrade
Switch(config-threshold)# value rate 9
Switch(config-threshold)# exit
Switch(config-t-list)# threshold name cvrd failure
Switch(config-threshold)# value rate 7
Switch(config-threshold)# exit
Switch(config-t-list)# exit
Switch(config)# interface waveethernetphy 10/0
Switch(config-if)# threshold-group cvrd-counters
```

Displaying the Alarm Threshold Configuration

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

Command	Purpose
<code>show threshold-list [name]</code>	Displays the threshold group configuration.
<code>show interfaces {waveethernetphy slot/subcard tengigethernetphy slot/subcard}</code>	Displays the interface configuration.

Examples

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

```
Switch# show threshold-list cvrd-counters

Threshold List Name: cvrd-counters
  Notification throttle timer : 5 (in secs)
  Threshold name : CVRD Severity : Degrade
  Value : 10e-9
  APS Trigger : Not set
  Threshold name : CVRD Severity : Failure
  Value : 10e-7
  APS Trigger : Not set
```

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

```
Switch# show interfaces waveethernetphy 10/0
WaveEthernetPhy10/0 is administratively down, line protocol is down
  Channel: 3      Frequency: 192.3 Thz   Wavelength: 1558.98 nm
  Active Wavepatch      : Wavepatch10/0/0
  Splitter Protected    : No
  Receive power level   : -8.38 dBm
  Laser shut down       : No
  Osc physical port     : No
  Wavelength used for inband management: No
  Loopback not set

Configured threshold Group(s): cvrd-counters
Threshold monitored for: 64b66b cvrd
SF set value: 10e-7 (1031 in 1 secs)
SD set value: 10e-9 (10 in 1 secs)
CDL HEC error count: 0
CRC error count: 0
Code violation and running disparity error count( 64b66b cvrd): 0
Number of times SF threshold exceeded: 0
Number of times SD threshold exceeded: 0

Defect Indication Status      : down
Configured Node Behavior      : None
Current Node Behavior         : Path Terminating
Defect Indication Receive     : FDI-H FDI-E
Defect Indication Transmit    : FDI-H FDI-E

MTU Size:      10232 bytes

Total Tx Frames Sent to N/W:  0
Tx Gen CDL Idle Frame:      540367537118

Rx Frames rcvd from N/W:     0
Rx IPG drpd pkts:           0
Rx Idle Packets :            0
Rx Oversize Frames :        0
Rx Undersize Frames :       0

Rx SII mismatch drpd data Frames :  0
Rx SII mismatch drpd idle Frames :  0

Last clearing of "show interface" counters never
Hardware is data_enabled_port
```

About Patch Connections

Because the mux/demux modules are passive devices, the Cisco ONS 15530 does not detect its optical patch connection configuration. For system management purposes, you must also configure the patch connection configuration using the CLI.

Configuring Patch Connections

To configure patch connections between link cards within the same shelf, use the following global configuration commands:

Command	Purpose
patch wavepatch <i>slot1/subcard1/port1</i> filter <i>slot2/subcard2/port2</i> or patch filter <i>slot1/subcard1/port1</i> wavepatch <i>slot2/subcard2/port2</i>	Configures the patch connection between a 2.5-Gbps ITU trunk card or 10-Gbps ITU trunk card and an OADM module.
patch thru <i>slot/subcard1</i> thru <i>slot/subcard2</i>	Configures the patch connection between two OADM modules.
patch wave <i>slot/subcard</i> oscfiler <i>slot/subcard</i> or patch oscfilter <i>slot/subcard</i> wave <i>slot/subcard</i>	Configures the patch connection between the wave interface on the OSC module and the oscfilter interface on the OADM module. This is only required if an OSC module is present.



Note

If you correctly patch your cards, **patch** command configuration is not necessary for the signal to pass from the client to the trunk fiber.

Example

The following example shows how to configure the patch connections between line cards in a shelf with two OSC cards in slot 4, two OADM modules with OSC in slot 0, and a splitter 2.5-Gbps ITU trunk card or 10-Gbps ITU trunk card in slot 3:

```
Switch# configure terminal
Switch(config)# patch thru 0/0 thru 0/1
Switch(config)# patch wave 4/0 oscfiler 0/0
Switch(config)# patch wave 4/1 oscfiler 0/1
Switch(config)# patch wavepatch 3/0/0 filter 0/0/1
Switch(config)# patch wavepatch 3/0/1 filter 0/1/1
```




Configuring VOA Module Interfaces

This chapter describes how to configure the VOA modules supported by the Cisco ONS 15530. These modules allow the Cisco ONS 15530 to extend the internodal distances and number of nodes supported for point-to-point, hubbed ring, and meshed ring topology networks.

This chapter includes the following sections:

- [About Variable Optical Attenuation, page 8-1](#)
- [Configuring VOA Module Interfaces, page 8-5](#)
- [Configuring Attenuation, page 8-5](#)
- [Displaying the Attenuation Configuration, page 8-7](#)
- [About Optical Thresholds, page 8-8](#)
- [Configuring Optical Receive Power Thresholds, page 8-8](#)



Note

To ensure the installed Cisco IOS software supports your hardware and provides the software features you wish to use, see the [“New and Changed Information” section on page xiii](#). Also refer to the “Hardware Supported” section and “Feature Set” section of the latest release notes for the Cisco ONS 15530.

About Variable Optical Attenuation

The attenuation typically occurs on the input side of the EDFA (erbium-doped fiber amplifier) so that the input power of each band transmitted to the EDFA is equalized. The VOA modules can also attenuate OSC channels, EDFA output (when preamplifying), or individual data channels.

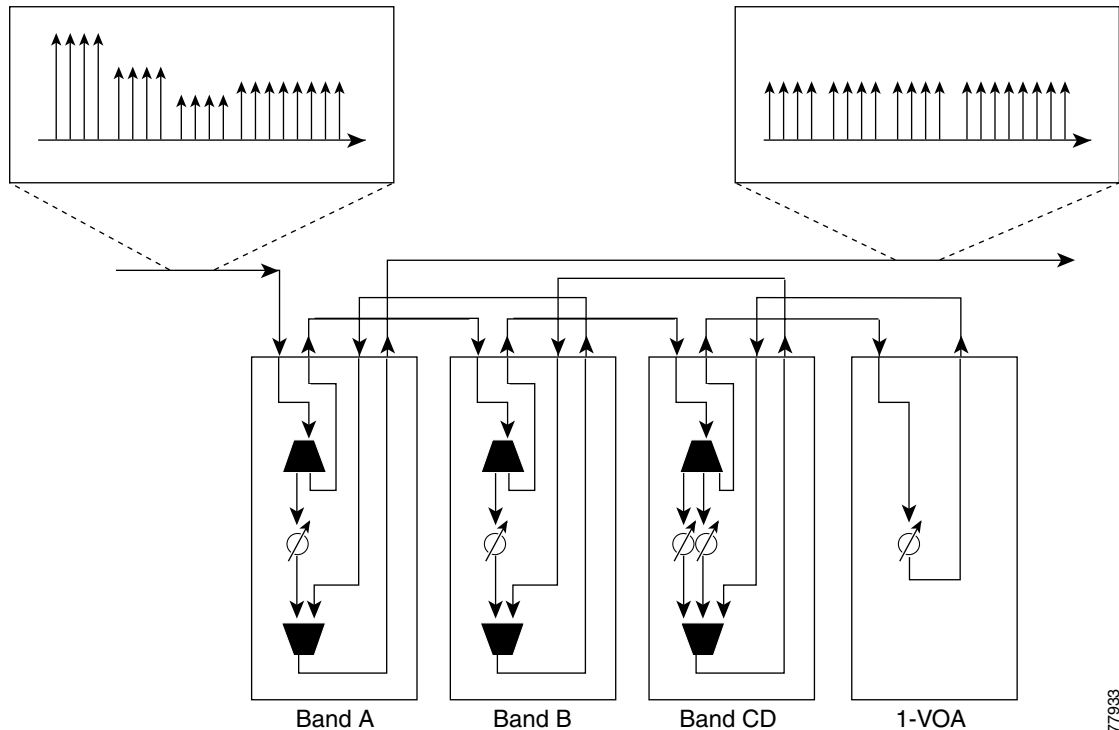
The Cisco ONS 15530 supports two types of VOA modules:

- PB-OE (per-band optical equalizer) modules
- WB-VOA (wide-band variable optical attenuator) modules

A PB-OE module selects one or two bands of channels to attenuate and passes on the rest of the signal. WB-VOA modules attenuate all the channels it receives.

[Figure 8-1](#) illustrates the use of PB-OE and WB-VOA modules to perform band based power equalization.

Figure 8-1 Four Band Equalization with Three Power Equalizers



77933

VOA Modules

The VOA modules are half-width modules inserted into a carrier motherboard installed in a Cisco ONS 15530 shelf. The carrier motherboards can be installed in slots 1 through 4 and 7 through 10. All optical connectors are located on the front panel and the connectors are angled and recessed.

Each carrier motherboard can hold up to two VOA modules. There are four types of VOA modules available:

- Single WB-VOA modules
- Dual WB-VOA modules
- Single band PB-OE modules
- Dual band PB-OE modules

Single WB-VOA Modules

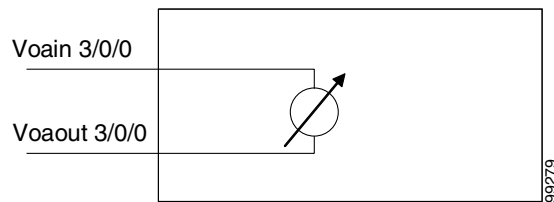
The single WB-VOA modules accept one signal and attenuate all frequencies within that signal. The signal can contain a single channel, such as the OSC, a band of channels, or multiple channel bands.

Single WB-VOA modules have two types of interfaces:

- Voain interfaces
- Voout interfaces

Figure 8-2 shows the interfaces for the single WB-VOA module.

Figure 8-2 Single WB-VOA Module Interfaces



Dual WB-VOA Modules

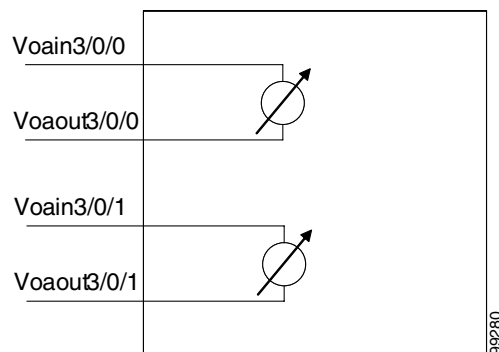
The dual WB-VOA modules consist of two WB-VOA units that each accepts one signal and attenuates all frequencies within that signal.

Dual WB-VOA modules have two types of interfaces:

- Voain interfaces
- Voayout interfaces

Figure 8-3 shows the interfaces for the dual WB-VOA module.

Figure 8-3 Dual WB-VOA Module Interfaces



Single Band PB-OE Modules

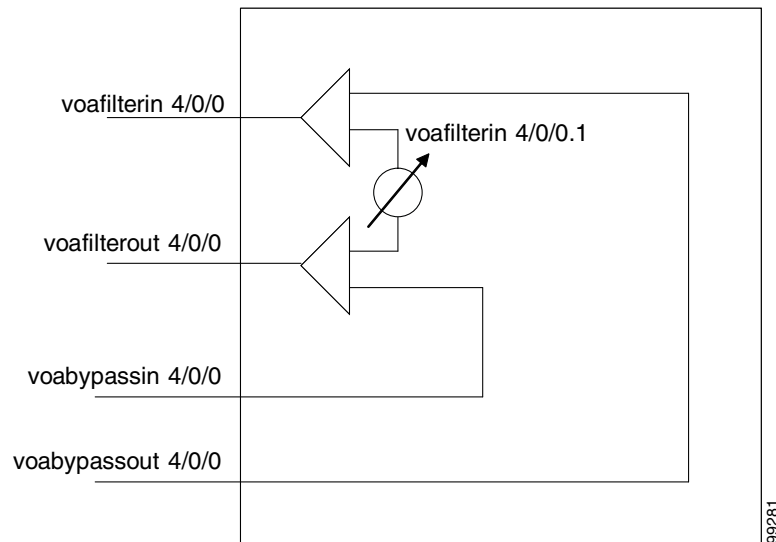
A single band PB-OE module accepts an incoming signal containing at least two bands, which are split by an optical filter into two components. The first component is attenuated and the second component is passed to another module where it can be attenuated and passed back to the original PB-OE. The PB-OE then recombines the two equalized components into a single signal and sends it out.

Single PB-OE modules have four types of interfaces:

- Voafilterin interfaces and subinterfaces
- Voafilterout interfaces
- Voabypassin interfaces
- Voabypassout interfaces

Figure 8-4 shows the interfaces for the single PB-OE module.

Figure 8-4 Single PB-OE Module Interfaces



Dual Band PB-OE

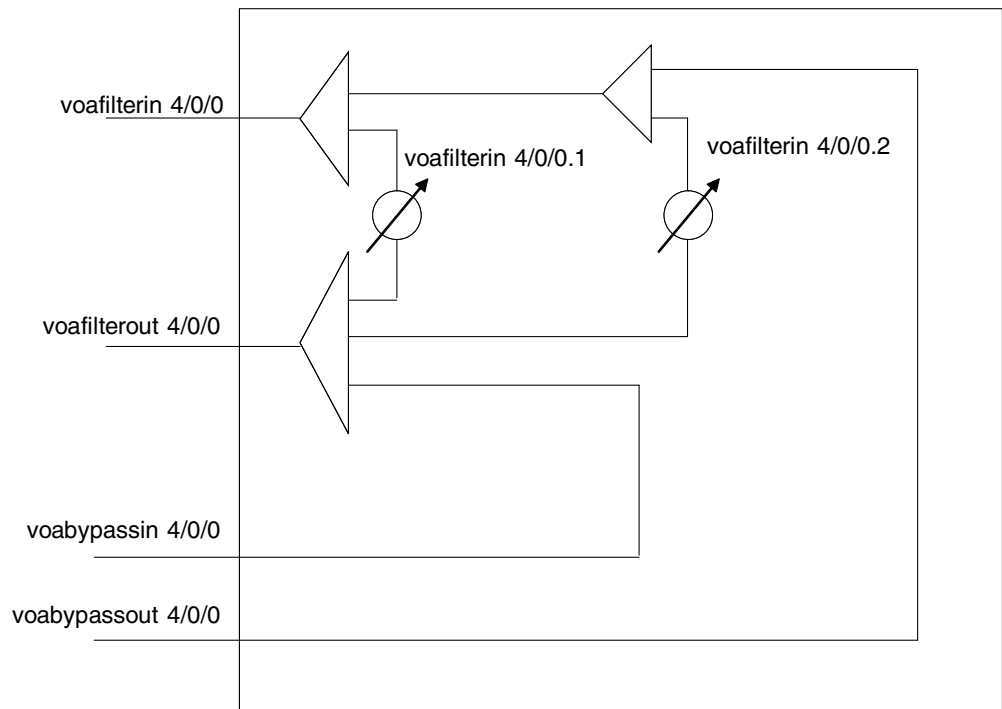
If two consecutive bands have to be attenuated, use a dual band PB-OE module. When more than two add bands are to be attenuated, multiple VOA modules can be cascaded. The dual band PB-OE supports bands AB, CD, EF, and GH. Use a dual band PB-OE module to equalize signals with at least two bands.

Dual PB-OE modules have four types of interfaces:

- Voafilterin interfaces and subinterfaces
- Voafilterout interfaces
- Voabypassin interfaces
- Voabypassout interfaces

Figure 8-5 shows the interfaces for the dual PB-OE module.

Figure 8-5 Dual PB-OE Module Interfaces



Configuring VOA Module Interfaces

The following steps describe the configuration tasks for optical amplification support on the Cisco ONS 15530:

-
- Step 1** Configure attenuation values.
 - Step 2** Configure alarm thresholds (optional).
 - Step 3** Configure topology neighbor information (optional).

For information on configuring topology neighbor information, see the [“Configuring Interfaces in the Network Topology”](#) section on page 12-21.

Configuring Attenuation

The Cisco ONS 15530 supports two types of attenuation, automatic and manual. The WB-VOA module allows both automatic and manual attenuation. The PB-OE module only allows manual attenuation.

For more information on configuring attenuation in an amplified network, refer to the [Cisco ONS 15530 Optical Turn-up and Test Guide](#) publication.

Configuring Automatic Attenuation

The WB-VOA modules support automatic attenuation. Once you set a desired signal power, the system checks every second until the signal power comes into attenuable range. Then the system sets the attenuation so that the signal transmits at the desired power value. The system waits 60 seconds before checking the signal power again and adjusting the attenuation if necessary. The system automatically adjusts the attenuation only if it is at least 0.5 dBm out of range.

To configure automatic attenuation on a WB-VOA module interface, perform the following steps:

	Command	Purpose
Step 1	Switch# configure terminal Switch(config)#	Enters global configuration mode.
Step 2	Switch(config)# interface voain slot/subcard/port Switch(config-if)#	Selects the WB-VOA module interface to configure and enters interface configuration mode.
Step 3	Switch(config-if)# optical attenuation automatic desired-power value	Specifies the automatic attenuation value in units of 0.1 dBm.



Note

Automatic attenuation and manual attenuation are mutually exclusive. Only one method can be active at a given time. If manual attenuation is in effect, the **optical attenuation automatic desired-power** command overrides that configuration.

Example

The following example shows how to configure automatic attenuation on a voain interface on a WB-VOA module:

```
Switch# configure terminal
Switch(config)# interface voain 1/0/0
Switch(config-if)# optical attenuation automatic desired-power 150
```

Configuring Manual Attenuation

The WB-VOA modules and PB-OE modules support manual configuration of attenuation. When you manually configure the attenuation, the interface attenuates at the value specified in the command.

To configure manually attenuation on a VOA module interface, perform the following steps:

	Command	Purpose
Step 1	Switch# show interfaces { voafilterin slot/subcard/port.subinterface voain slot/subcard/port } attenuation desired-power value	Shows the attenuation value necessary to achieve the desired power value.
Step 2	Switch# configure terminal Switch(config)#	Enters global configuration mode.

	Command	Purpose
Step 3	Switch(config)# interface { voafilterin <i>slot/subcard/port.subinterface</i> voain <i>slot/subcard/port</i> }	Selects the VOA module interface to configure and enters interface configuration mode.
	Switch(config-if)#	
Step 4	Switch(config-if)# optical attenuation manual <i>value</i>	Specifies the manual attenuation value in units of 0.1 dBm.

**Note**

Automatic attenuation and manual attenuation are mutually exclusive. Only one method can be active at a given time. If automatic attenuation is in effect, the **optical attenuation manual** command overrides that configuration.

Example

The following example shows how to manually configure attenuation on a voafilterin subinterface on a PB-OE module:

```
Switch# configure terminal
Switch(config)# interface voafilterin 1/0/0.1
Switch(config-subif)# optical attenuation manual 20
```

The following example shows how to calculate and configure attenuation on a voain interface on a WB-VOA module:

```
Switch# show interfaces voain 1/0/0 attenuation desired-power 0
Current Output Power:                10.0dBm
Desired Output Power:                 0.0dBm
Minimum settable Attenuation:         3.4dB
Maximum settable Attenuation:         30.0dB
Current set Attenuation:               3.4dB (default)
Attenuation needed to achieve Desired Output Power:13.4dB
Switch# configure terminal
Switch(config)# interface voain 1/0/0
Switch(config-if)# optical attenuation manual 13.4
```

Displaying the Attenuation Configuration

To display the attenuation configuration, use the following EXEC command:

Command	Purpose
show interfaces { voafilterin <i>slot/subcard/port.subinterface</i> voain <i>slot/subcard/port</i> }	Displays the VOA module interface configuration.

Example

The following example shows how to display the attenuation configuration of a voafilterin subinterface:

```
Switch# show interfaces voafilterin 9/0/0.1
voaFilterIn9/0/0.1 is up, line protocol is up
Hardware is voaFilterIn Port
Port Transmit (Tx) Support:          False
Port Receive (Rx) Support:           True
```

```

VOA This Port operates on:      2
Attenuation Mode:              manual
Minimum settable Attenuation:  3.7dB
Maximum settable Attenuation:  30.0dB
→ Current set Attenuation:      3.7dB (default)
Light Quality:                 Good/In Range
Current Output Power:          -0.5dBm
Low Alarm Threshold Severity:  major (default)
Low Warning Threshold:         -27.0dBm (default)
Low Warning Threshold Severity: not alarmed (default)
High Warning Threshold:        9.0dBm (default)
High Warning Threshold Severity: not alarmed (default)
High Alarm Threshold:          11.0dBm (default)
High Alarm Threshold Severity: major (default)

```

The following example shows how to display the attenuation configuration of a voain interface:

```

Switch# show interfaces voain 9/0/0
voain9/0/0 is up, line protocol is up
  Hardware is voaIn Port
  Port Transmit (Tx) Support:    False
  Port Receive (Rx) Support:     True
  VOA This Port operates on:     1
→ Attenuation Mode:              manual
  Minimum settable Attenuation:  1.7dB
→ Maximum settable Attenuation:  30.0dB
  Current set Attenuation:        15.0dB
  Light Quality:                 Good/In Range
  Current Output Power:          -12.1dBm
  Low Alarm Threshold Severity:  major (default)
  Low Warning Threshold:         -27.0dBm (default)
  Low Warning Threshold Severity: not alarmed (default)
  High Warning Threshold:        9.0dBm (default)
  High Warning Threshold Severity: not alarmed (default)
  High Alarm Threshold:          11.0dBm (default)
  High Alarm Threshold Severity: major (default)

```

About Optical Thresholds

You can configure optical thresholds on the VOA module interfaces that issue alarm messages to the system if the optical thresholds are exceeded. Every second, the monitoring facility updates the counters that correspond to the alarm thresholds. When the signal degrades, or fails entirely, the system issues alarms to the console. These alarms can help isolate failures in the system and in the network.

Configuring Optical Receive Power Thresholds

The VOA modules have optical receive power thresholds monitored by the Cisco ONS 15530. This section describes four types of alarm threshold configuration procedures:

- Low Power Alarm
- Low Power Warning
- High Power Warning
- High Power Alarm

Low power warnings are raised when the received optical power drifts too close to LOL (loss of light). Low power alarms show a critical condition of LOL. High power warnings are raised when the received optical power drifts too close to high power alarm conditions. High power alarm are raised when received optical power exceeds the receiver saturation threshold.

To configure power thresholds on VOA module interfaces, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface { voafilterin <i>slot/subcard/port.subinterface</i> voain <i>slot/subcard/port</i> }	Selects the VOA module interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# optical threshold power receive after-attenuation { low high } { alarm warning } <i>value</i> [severity { critical major minor not alarmed not reported }]	Specifies the threshold value in units of 0.1 dBm. The default values are as follows: Low alarm: -29 dBm Low warning: -27 dBm High warning: 9 dBm High alarm: 11 dBm Alarm severity: major Warning severity: not alarmed

Example

The following example shows how to manually configure an optical threshold on a voafilterin subinterface on a PB-OE module:

```
Switch# configure terminal
Switch(config)# interface vofilterin 1/0/0.1
Switch(config-subif)# optical threshold power receive after-attenuation low alarm -210
```

The following example shows how to configure an optical threshold on a voain interface on a WB-VOA module:

```
Switch# configure terminal
Switch(config)# interface voain 1/0/0
Switch(config-if)# optical threshold power receive after-attenuation high alarm -200
```

Displaying the Optical Threshold Configuration

To display the configuration of an optical threshold for a VOA module interface, use the following EXEC commands:

Command	Purpose
show interfaces { voafilterin <i>slot/subcard/port.subinterface</i> voain <i>slot/subcard/port</i> }	Displays the VOA module interface configuration.

Example

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

```
Switch# show interfaces vofilterin 2/1/0.2
vofilterIn2/1/0.2 is up, line protocol is up
```

```

Hardware is voaFilterIn Port
Port Transmit (Tx) Support:      False
Port Receive (Rx) Support:      True
VOA This Port operates on:      1
Attenuation Mode:                manual
Minimum settable Attenuation:    3.7dB
Maximum settable Attenuation:    30.0dB
Current set Attenuation:         20.0dB
Light Quality:                   Low Warning Threshold Exceeded
Current Output Power:            -16.3dBm
Low Alarm Threshold:             -20.0dBm
Low Alarm Threshold Severity:    major (Default Value)
Low Warning Threshold:          -15.0dBm
Low Warning Threshold Severity:  not-alarm (Default Value)
High Warning Threshold:         -10.0dBm
High Warning Threshold Severity: not-alarm (Default Value)
High Alarm Threshold:           -5.0dBm
High Alarm Threshold Severity:   major (Default Value)

```

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

```

Switch# show interfaces voain 7/1/0
voaIn7/1/0 is up, line protocol is down
Hardware is voaIn Port
Port Transmit (Tx) Support:      False
Port Receive (Rx) Support:      True
VOA This Port operates on:      1
Attenuation Mode:                manual
Minimum settable Attenuation:    1.7dB
Maximum settable Attenuation:    30.0dB
Current set Attenuation:         1.7dB
Light Quality:                   Loss of Light/Low Alarm Threshold Exceeded
Current Output Power:            -256.0dBm
Low Alarm Threshold:             -29.0dBm (Default Value)
Low Alarm Threshold Severity:    major (Default Value)
Low Warning Threshold:          -20.0dBm
Low Warning Threshold Severity:  not-alarm (Default Value)
High Warning Threshold:         -5.0dBm
High Warning Threshold Severity: not-alarm (Default Value)
High Alarm Threshold:           0.0dBm
High Alarm Threshold Severity:   major (Default Value)

```




Configuring PSM Interfaces

This chapter describes how to configure PSM (protection switch module) interfaces and patch connections on the Cisco ONS 15530. This chapter includes the following sections:

- [Enabling Wdmsplit Interfaces, page 9-1](#)
- [Configuring Trunk Fiber Based Protection, page 9-2](#)
- [About Switchovers and Optical Power Thresholds, page 9-3](#)
- [Configuring Optical Power Thresholds, page 9-7](#)
- [Configuring Patch Connections, page 9-9](#)
- [Configuring Wdmsplit Interfaces in the Network Topology, page 9-10](#)



Note

To ensure the installed Cisco IOS software supports your hardware and provides the software features you wish to use, see the “[New and Changed Information](#)” section on [page xiii](#). Also refer to the “Hardware Supported” section and “Feature Set” section of the latest release notes for the Cisco ONS 15530.

Enabling Wdmsplit Interfaces

To enable the PSM wdmsplit interfaces, perform the following tasks, starting in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface wdmsplit slot/subcard/0 Switch(config-if)#	Specifies the west wdmsplit interface and enters interface configuration mode.
Step 2	Switch(config-if)# no shutdown	Enables the interface.
Step 3	Switch(config-if)# exit Switch(config)#	Returns to global configuration mode.
Step 4	Switch(config)# interface wdmsplit slot/subcard/1 Switch(config-if)#	Specifies the east wdmsplit interface and enters interface configuration mode.
Step 5	Switch(config-if)# no shutdown	Enables the interface.

Example

The following example shows how to enable wdmsplit interfaces:

```
Switch(config)# interface wdmsplit 0/0/0
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# interface wdmsplit 0/0/1
Switch(config-if)# no shutdown
```

Displaying Wdmsplit Interface Information

The following example shows how to display wdmsplit interface information.

```
Switch# show interface wdmsplit 0/0/0
WdmSplit0/0/0 is down, line protocol is down
  Status                :Active
  Signal quality         :Loss of light
  Received power         :< -32.00 dBm (8E)
  Threshold Value        :-22.00 dBm (8CE)

  Optical threshold monitored for :Receive Power (in dBm)
  Threshold exceeded for :Low Warning and Low Alarm
  Low alarm value        = -22.0 dBm (default)
  Low Alarm Severity     = major
  Low warning value      = -18.0 dBm (default)
  Low Warning Severity   = not alarmed
  Hardware is split wavelength_add_drop
```

Configuring Trunk Fiber Based Protection

To configure trunk fiber protection on the wdmsplit interfaces, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# redundancy Switch(config-red)#	Enters redundancy mode.
Step 2	Switch(config-red)# associate group name Switch(config-red-aps)#	Specifies an APS group name and enters APS configuration mode. Note The group name is case sensitive.
Step 3	Switch(config-red-aps)# aps working wdmsplit slot/subcard/port	Configures the working path interface.
Step 4	Switch(config-red-aps)# aps protection wdmsplit slot/subcard/port	Configures the protection path interface.
Step 5	Switch(config-red-aps)# aps message-channel {auto-select inband dcc ip osc} far-end name	Configures the name of the corresponding APS group on the other node in the topology.
Step 6	Switch(config-red-aps)# aps enable	Enables APS activity between the interfaces.

For more information on configuring APS and trunk fiber based protection, refer to [Chapter 10, “Configuring APS.”](#)

Examples

The following example shows how to configure trunk fiber protection:

```
Switch(config)# redundancy
Switch(config-red)# associate group psm-group
Switch(config-red-aps)# aps working wdmsplit 0/1/0
Switch(config-red-aps)# aps protection wdmsplit 0/1/1
Switch(config-red-aps)# aps message-channel auto-select far-end group-name psm-group
Switch(config-red-aps)# aps enable
```

Displaying Trunk Fiber Protection Configuration

To display the trunk fiber configuration, use the following EXEC command:

Command	Purpose
show aps {detail group name interface wavepatch slot/subcard/port}	Displays detailed APS configuration information for groups and interfaces.
	Note Group names are case sensitive.

Examples

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

```
Switch# show aps group psm-group
APS Group psm-group :

  architecture.:1+1, remote prov:unknown
  span.....:end-to-end
  prot. mode...:network side wdm 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
  msg-channel...:auto (down), psm-group
  created.....:2 minutes
  auto-failover:disabled
  transmit k1k2:sf-lp, 0, 0, 1+1, uni
  receive k1k2:no-request, 0, 0, unknown, unknown
  switched chan:0
  protection(0):WdmSplit0/0/1 (STANDBY - UP)
    :channel request:sf-lp
    :switchover count:1
    :last switchover:0 minutes
  working...(1):WdmSplit0/0/0 (ACTIVE - UP)
    :channel request:sf-lp
    :switchover count:1
    :last switchover:0 minutes
```

About Switchovers and Optical Power Thresholds

The switchovers for trunk fiber protection on the PSM are controlled by an optical power threshold value set in the CLI. The value to set is determined by the characteristics of the point-to-point topology. The PSM supports the following types of point-to-point topologies:

- Unamplified

- Post-amplified
- Pre-amplified and post-amplified

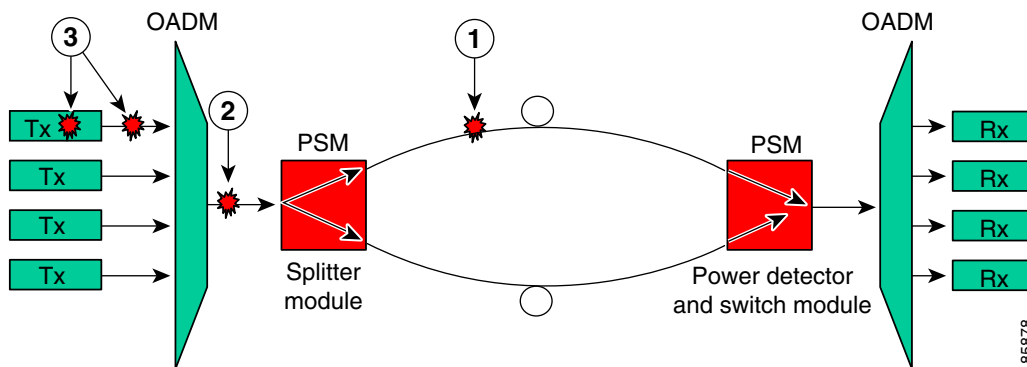
**Note**

Due to the cumulative effect of the noise from the EDFAs (erbium-doped fiber amplifiers), the PSM cannot support point-to-point topologies with more than two EDFAs on the trunk fiber. For topologies with three or more EDFAs on the trunk fiber, use splitter based protection.

Unamplified Topologies

A topology without amplification is the simplest case. Figure 9-1 shows an unamplified topology and the locations where failures can occur.

Figure 9-1 Point-to-Point Topology Without Amplification



1	Trunk fiber cut	3	Individual channel failures
2	OADM module-to-PSM patch cable cut		

**Note**

The minimum channel power into the EDFA must be -15 dBm or higher.

The switching behavior for the failures is as follows:

- Trunk fiber cut

The receive power on the active path drops below the minimum detectable level (-31 dBm) and the PSM switches over to the standby path.
- OADM module-to-PSM patch cable cut

In this case, the receive power on both the active and standby paths drops below the minimum detectable level. However, a switchover will occur if the auto-failover is enabled in the hardware. Since the system monitors the standby signal at 1 second intervals, the system might not detect the standby signal failure before the switchover occurs. After this switchover, no further switchovers occur.
- Individual channel failures

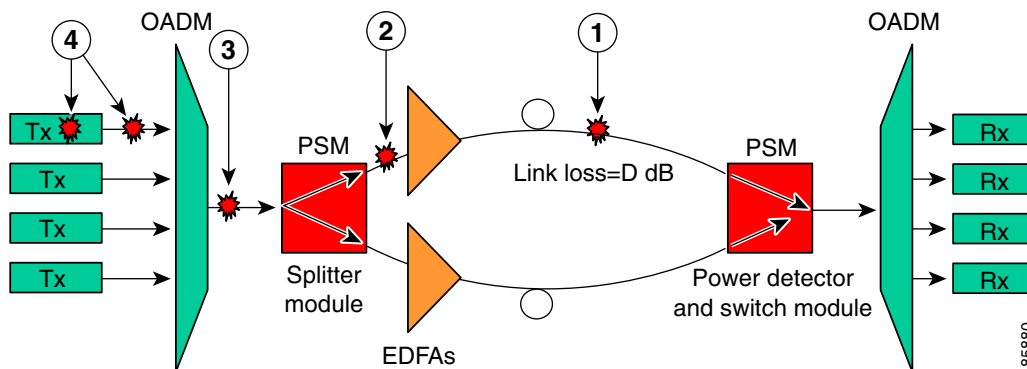
No switchover occurs because the change in the channel power is less than 15 dB.

The recommended low alarm threshold value for this topology is -28 dBm and the low warning threshold is at least -26 dBm.

Post-Amplified Topologies

Figure 9-2 shows an example topology with post-amplification and the locations where failures can occur.

Figure 9-2 Point-to-Point Topology with Post-Amplification



1	Trunk fiber cut	3	OADM module-to-PSM patch cable cut
2	PSM-to-EDFA patch cable cut	4	Individual channel failures



Note

The minimum channel power into the EDFA must be -15 dBm or higher.

The switching behavior for the failures is as follows:

- Trunk fiber cut

The receive power on the active path drops below the minimum detectable level (-31 dBm), and the PSM switches over to the standby path.
- PSM-to-EDFA patch cable cut

The EDFA generates -9 dBm of noise on the active path so the PSM receives $(-9 - D)$ dBm signal power where D is the link loss between the EDFA and the PSM receiver. If the low alarm optical threshold is set correctly, the PSM switches over to the standby path.
- OADM module-to-PSM patch cable cut

The EDFA generates -9 dBm of noise on both paths so the PSM receives $(-9 - D)$ dBm signal power where D is the link loss between the EDFA and the PSM receiver. If auto-failover is enabled and the low alarm optical threshold is set correctly, the PSM switches to the standby path before it detects that the standby path has also failed. No further switchovers occur.
- Individual channel failures

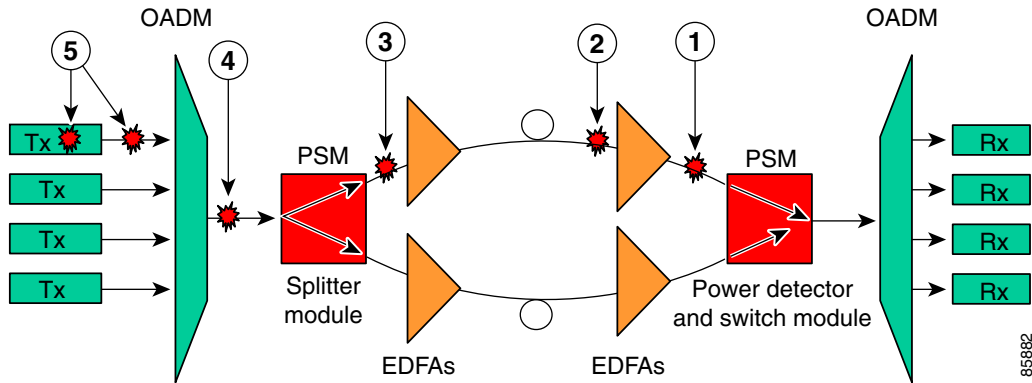
No switchover occurs because the change in the channel power is less than 15 dB.

The recommended value for the low alarm optical threshold is $(-6 - D)$ dBm, and the low warning threshold is at least 2 dB higher.

Post-Amplified and Pre-amplified Topologies

Figure 9-3 shows a topology with post-amplification and pre-amplification and the locations where failures can occur.

Figure 9-3 Point-to-point Topology with Post-Amplification and Pre-amplification



1	EDFA-to-PSM patch cable cut	4	OADM module-to-PSM patch cable cut
2	Trunk fiber cut	5	Individual channel failures
3	PSM-to-EDFA patch cable cut		



Note

The minimum channel power into the EDFA must be -15 dBm or higher.

The switching behavior for the failures is as follows:

- EDFA-to-PSM patch cable cut

The receive power on the active path drops below the minimum detectable level (-31 dBm) and the PSM switches over to the standby path.
- Trunk fiber cut

The EDFA generates -9 dBm of noise so the PSM receives $(-9 - L)$ dBm signal power, where L is the output attenuation from the EDFA. The PSM switches over to the standby path if the low alarm threshold is correctly configured.
- PSM-to-EDFA patch cable cut

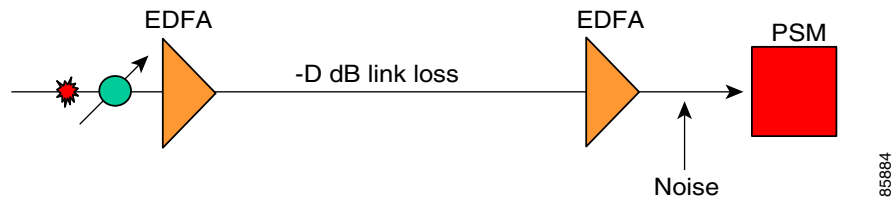
The receive power drops but not below the minimum detectable level because of the cumulative noise from the two EDFAs. The PSM switches over to the standby signal if the low alarm threshold is correctly configured.
- OADM module-to-PSM patch cable cut

The receive power drops but not below the minimum detectable level because of the cumulative noise from the two EDFAs. If auto-failover is enabled, the PSM switches to the standby path before it detects that the standby path has also failed. No further switchovers occur.
- Individual channel failures

No switchover occurs because the change in the channel power is less than 15 dB.

Figure 9-4 shows an example topology and the locations where failures can occur.

Figure 9-4 Failure Scenario with Noise from Two EDFAs



You can calculate the noise using the following formula:

$$10 \text{ dB} * \log(10^{((-9)/10)} + 10^{((-9-D+17)/10)}) \text{ dB} - L \text{ dB}$$

where D is the link loss between the EDFAs and L is equal to 17 minus the configured gain on the EDFA closest to the PSM receiver.

The recommended value for the low alarm optical threshold is the calculated noise value plus 3 dBm.

Set the low warning threshold at least 2 dB higher.

Configuring Optical Power Thresholds

The optical power thresholds provide a means of monitoring the signal power received from the active trunk fiber path. Two types of thresholds are provided:

- Low alarm
- Low warning

When the low alarm threshold is crossed on the active path, the PSM switches over to the standby path. When either of the thresholds are crossed, the system sends messages to the console and generates traps, if traps are enabled.

To configure optical power thresholds for wdmsplit interfaces on a PSM, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface wdmsplit slot/subcard/0 Switch(config-if)#	Selects wdmsplit interface that carries traffic for the west direction and enters interface configuration mode.
Step 2	Switch(config-if)# optical threshold power receive {low high} {alarm warning} value [severity {critical major minor not alarmed not reported}]	Specifies the optical power threshold value in units of 0.1 dBm. The range is -280 to 0. The default values are as follows: Low alarm: -22 dBm Low warning: -20 dBm Alarm severity: major Warning severity: not alarmed
Step 3	Switch(config-if)# exit Switch(config)#	Returns to global configuration mode.

	Command	Purpose
Step 4	Switch(config)# interface wdmsplit slot/subcard/1 Switch(config-if)#	Selects the wdmsplit interface that carries traffic for the east direction and enters interface configuration mode.
Step 5	Switch(config-if)# optical threshold power receive {low high} {alarm warning} value [severity {critical major minor not alarmed not reported}]	Specifies the optical power threshold value in units of 0.1 dBm.

Examples

The following example shows how to configure optical power thresholds for wdmsplit interfaces on a PSM:

```
Switch(config)# interface wdmsplit 0/1/0
Switch(config-if)# optical threshold power receive low alarm -27
Switch(config-if)# optical threshold power receive low warning -25
Switch(config-if)# exit
Switch(config)# interface wdmsplit 0/1/1
Switch(config-if)# optical threshold power receive low alarm -26
Switch(config-if)# optical threshold power receive low warning -24
```

Displaying Optical Power Threshold Configuration

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

Command	Purpose
show interfaces wdmsplit slot/subcard/port	Displays interface information.

Example

The following example shows how to display the optical threshold configuration for an interface:

```
Switch# show interfaces wdmsplit 0/1/0
WdmSplit0/1/0 is administratively down, line protocol is down
  Status                :Active
  Received power         :0.00 dBm (EF9)
  Threshold Value        :-22.00 dBm (8CE)

  Optical threshold monitored for :Receive Power (in dBm)
  Low alarm value        = -22.0 dBm (default)
  Low Alarm Severity     = major
  Low warning value      = -20.0 dBm (default)
  Low Warning Severity   = not alarmed
  High alarm value       = -2.0 dBm (default)
  High Alarm Severity    = major
  High warning value     = -4.0 dBm (default)
  High Warning Severity  = not alarmed
  Hardware is split wavelength_add_drop
```


Configuring Patch Connections

To configure patch connections between a PSM and an OADM module, use the following global configuration command:

Command	Purpose
<pre>patch wdm slot/subcard1 wdmrelay slot/subcard2/port</pre> or <pre>patch wdmrelay slot/subcard1/port wdm slot/subcard2</pre>	Configures the patch connection between a PSM and an OADM module.
<pre>patch wavepatch slot/subcard1/port wdmrelay slot/subcard2/port</pre> or <pre>patch wdmrelay slot/subcard1/port wavepatch slot/subcard1/port</pre>	Configures the patch connection between a PSM and a 2.5-Gbps transponder module or 10-GE transponder module. Note If you connect to a transponder line card, you must use IP to manage your network topology. If you connect to an ITU trunk card, you must use the ethernetdcc interface to manage your network topology.



Note

When the patch between a wdm interface and a wdmrelay interface is configured, CDP topology learning on the wdm interface is disabled.

Example

The following example shows how to configure the patch connections between a PSM and an OADM module:

```
Switch# configure terminal
Switch(config)# patch wdm 0/0 wdmrelay 0/1/0
```

Displaying Patch Connections

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

Command	Purpose
<code>show patch [detail]</code>	Displays the patch connections.
<code>show interfaces { wdm slot/subcard1 wdmrelay slot/subcard2/port wavepatch slot/subcard1/port }</code>	Displays the interface information.

Example

The following example shows the patch connections:

```
Switch# show patch
Patch Interface      Patch Interface      Type      Dir      Error
-----
Wdm0/0              WdmRelay0/1/0       USER      Both
```

```
Switch# show interfaces wdm0/0
Wdm0/0 is up, line protocol is up
```

```
Patched Interface(s) :WdmRelay0/1/0
Wdm Hw capability:N/A
Num of Wavelengths Add/Dropped:5
List of Wavelengths:0, 13, 14, 15, 16
Hardware is wavelength_add_drop
```

Configuring Wdmsplit Interfaces in the Network Topology

The wdmsplit interfaces on a PSM do not support CDP and must be manually configured in the network topology.



Note

The patch connection between the PSM and the OADM module, ITU trunk card, or transponder line card must be configured correctly. For more information on configuring the patches for these interfaces, see the [“Configuring Patch Connections” section on page 9-9](#).



Note

When a patch connection between an OADM module and a PSM is configured, topology learning on the wdm interface is disabled.

To add wdmsplit interfaces to the network topology, perform the following steps on the wdmsplit interfaces on both the nodes in the point-to-point network topology, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface wdmsplit <i>slot/subcard/0</i> Switch(config-if)#	Selects the west wdmsplit interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# topology neighbor { name <i>node-name</i> ip-address <i>node-ip-address</i> mac-address <i>node-mac-address</i> } { port { name <i>port-name</i> ip-address <i>port-ip-address</i> mac-address <i>port-mac-address</i> } }	Configures the network topology information for the neighboring node.
Step 3	Switch(config-if)# topology neighbor agent ip-address <i>ip-address</i>	Specifies the IP address of the network topology agent on the neighboring node.
Step 4	Switch(config-if)# exit Switch(config)#	Returns to interface configuration mode.
Step 5	Switch(config)# interface wdmsplit <i>slot/subcard/1</i> Switch(config-if)#	Selects the east wdmsplit interface to configure and enters interface configuration mode.

	Command	Purpose
Step 6	Switch(config-if)# topology neighbor { name <i>node-name</i> ip-address <i>node-ip-address</i> mac-address <i>node-mac-address</i> } { port { name <i>port-name</i> ip-address <i>port-ip-address</i> mac-address <i>port-mac-address</i> } }	Configures the network topology information for the neighboring node.
Step 7	Switch(config-if)# topology neighbor agent ip-address <i>ip-address</i>	Specifies the IP address of the network topology agent on the neighboring node.

Example

The following example shows how to add wdmsplit interfaces to the network topology:

```
Switch(config)# interface wdmsplit 1/1/0
Switch(config-if)# topology neighbor name NodeB port name wdmsplit1/1/0
Switch(config-if)# topology neighbor agent ip-address 10.1.1.1
Switch(config-if)# exit
Switch(config)# interface wdmsplit 1/1/1
Switch(config-if)# topology neighbor name NodeB port name wdmsplit1/1/1
Switch(config-if)# topology neighbor agent ip-address 10.1.1.1
```

Displaying Topology Information for Wdmsplit Interfaces

To display the topology information for wdmsplit interfaces, use the following EXEC command:

Command	Purpose
show topology neighbor	Displays network topology information.

Example

The following example shows how to display the topology information:

```
Switch# show topology neighbor
Physical Topology:
```

Local Port	Neighbor Node	Neighbor Port	Link Dirn
-----	-----	-----	-----
WdmSplit0/1/0	PSM-2	wdms0/1/0	Both
WdmSplit0/1/1	PSM-2	wdms0/1/1	Both



Configuring APS

This chapter describes how protection is implemented on the Cisco ONS 15530. It also describes how to configure splitter protection and line card protection with APS (Automatic Protection Switching). This chapter contains the following sections:

- [About APS, page 10-2](#)
- [About Splitter Protection, page 10-2](#)
- [Configuring Splitter Protection, page 10-5](#)
- [About Line Card Protection, page 10-7](#)
- [About Client Based Line Card Protection, page 10-7](#)
- [About Y-Cable Line Card Protection, page 10-9](#)
- [Configuring Y-Cable Based Line Card Protection, page 10-11](#)
- [About Switch Fabric Based Line Card Protection, page 10-13](#)
- [Configuring Switch Fabric Based Line Card Protection, page 10-14](#)
- [About Trunk Fiber Based Protection, page 10-16](#)
- [Configuring Trunk Fiber Protection, page 10-17](#)
- [About Redundant Switch Fabric Protection, page 10-18](#)
- [Configuring APS Group Attributes, page 10-19](#)
- [About Switchovers and Lockouts, page 10-29](#)
- [Requesting a Switchover or Lockout, page 10-30](#)
- [Clearing Switchovers and Lockouts, page 10-31](#)



Note

To ensure the installed Cisco IOS software supports your hardware and provides the software features you wish to use, see the “[New and Changed Information](#)” section on [page xiii](#). Also refer to the “[Hardware Supported](#)” section and “[Feature Set](#)” section of the latest release notes for the Cisco ONS 15530.

About APS

APS provides protection against signal transmission failure. The Cisco ONS 15530 supports the following APS features:

- 1+1 path protection
- Splitter protection
- Line card protection
 - Client based
 - Y-cable based
 - Switch fabric based
- Trunk fiber protection
- Redundant switch fabric protection
- Bidirectional and unidirectional path switching

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

**Note**

For an [animated description](#) of the APS implementation on the Cisco ONS 15530, go to the following URL:

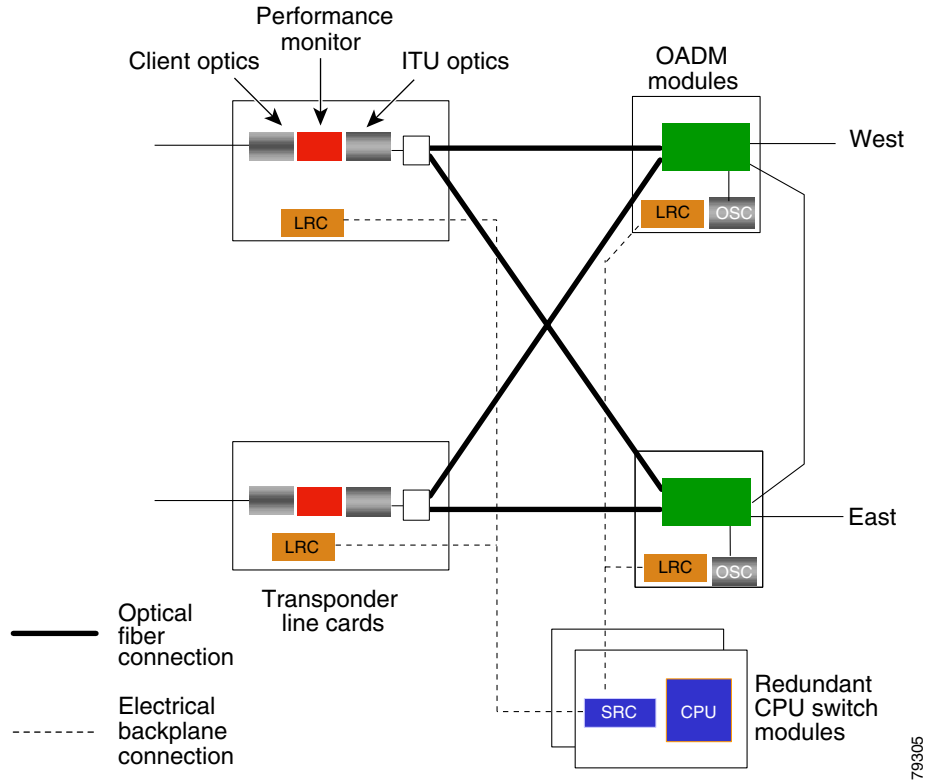
<http://www.cisco.com/mm/dyngraph/APS15530.html>

About Splitter Protection

Splitter protection on the Cisco ONS 15530 provides protection against facility failure, such as trunk fiber cuts, but not ITU laser failures or client equipment failures. Splitter line cards internally replicate the client optical signal and transmit it to both OADM modules. The Cisco ONS 15530 supports splitter versions of the transponder line card, the 2.5-Gbps ITU trunk card, and the 10-Gbps ITU trunk card.

[Figure 10-1](#) shows splitter protection with a transponder line card.

Figure 10-1 Splitter Protection Scheme

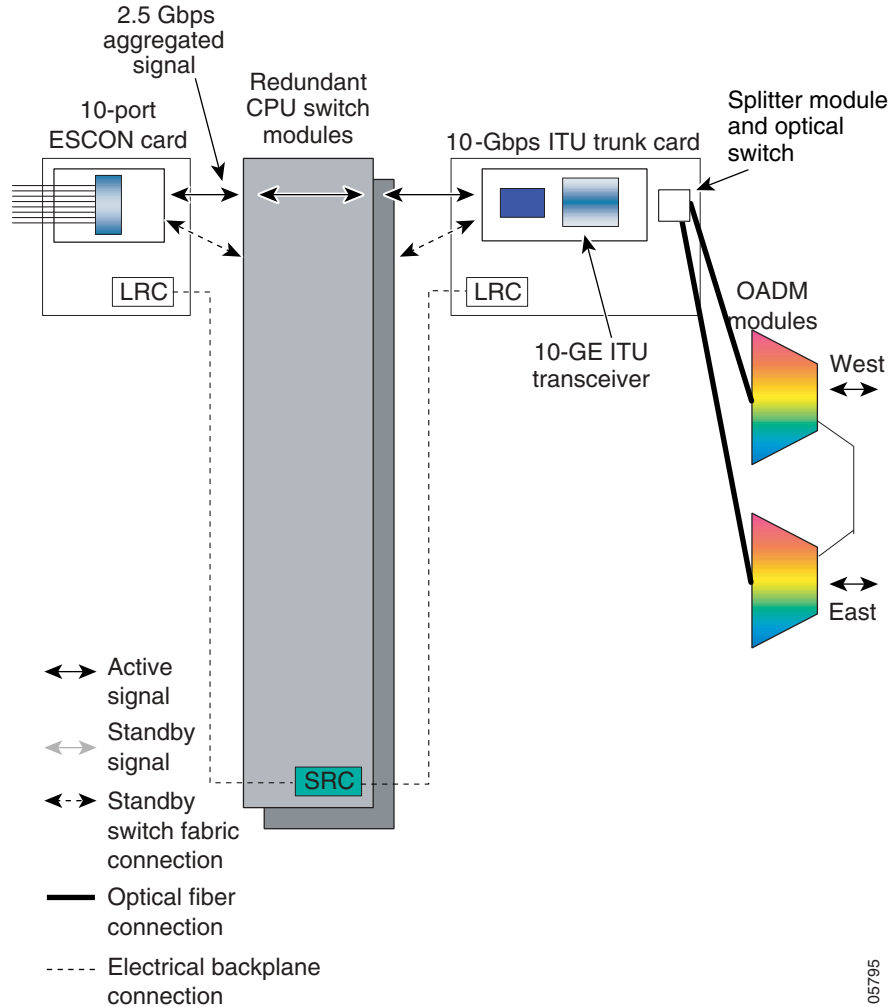


79305

On the ITU side, a fiber pair, with one receive fiber and one transmit fiber, connects to the OADM module transmitting in the west direction. Another fiber pair connects to the OADM module transmitting in the east direction. A 2x2 switch module on the line card receives both signals from the trunk fiber pairs and selects one as the active signal. When a signal failure is detected, the line card switches over to receive the standby signal. The standby signal then becomes the active signal.

Figure 10-2 shows splitter protection with a 10-Gbps ITU trunk card.

Figure 10-2 Cisco ONS 15530 Trunk Card Splitter Protection



Considerations for Using Splitter Protection

The following considerations apply when considering the use of splitter protection:

- Splitter protection does not protect against failure of the splitter line card. Splitter protection also does not protect against failure of a client line card or of the client equipment.

To protect against laser failure for transponder line cards, 2.5-Gbps ITU trunk card, and 10-Gbps ITU trunk cards, use y-cable protection as described in the [“About Line Card Protection”](#) section on page 10-7 and the [“Configuring Y-Cable Based Line Card Protection”](#) section on page 10-11. To protect against ESCON card failure or the client equipment, implement protection on the client equipment instead.

- A fully provisioned single shelf configuration can support 4 channels in splitter protection mode. A fully provisioned multiple shelf configuration can support up to 32 channels in splitter protection mode.

For more information about multiple shelf nodes, see [Chapter 11, “Configuring Multiple Shelf Nodes.”](#)

- Splitter protection supports revertive behavior. With revertive APS, the signal automatically switches back to the working path after the receive signal defect has been corrected and the wait to restore timer is expired. The default behavior is nonrevertive. When defects on the working channel are cleared, a wait to restore timer is started. Once this timer expires, the working channel becomes the active channel if no other problems occur on the working path.
- For interfaces configured for splitter APS and either Sysplex ETR or Sysplex CLO protocol encapsulation, configure bidirectional path switching to ensure proper functioning of these protocols.
- For bidirectional path switching to function on the transponder line cards, the OSC is required for exchanging APS channel protocol messages. For bidirectional path switching on the 2.5-Gbps ITU trunk card or 10-Gbps ITU trunk card, either the in-band message channel, the OSC, or the IP management connection can be used for the APS channel protocol messages.

For detailed information on shelf configuration rules, refer to the [Cisco ONS 15530 Planning Guide](#).

Configuring Splitter Protection

The following steps describe the tasks required to configure splitter protection:

-
- Step 1** Determine the number of channels you will deploy to transport client data.
 - Step 2** Ensure that the correct line cards are inserted in slots 1 through 4 or 7 through 10.
 - Step 3** Ensure that the line cards and modules are correctly interconnected with the external optical patch cables. For ring topologies, connect the thru interface on one OADM to the thru interface on the other.
 - Step 4** Configure the interfaces and the patch connections from the CLI (command-line interface).
 - Step 5** Configure APS from the CLI.
-



Caution

Do not enable laser safety control with splitter protection. If you configure the system with splitter protection and enable laser safety control, the transmit laser shuts down when an open fiber occurs on one transport fiber and signal transmission to the client is interrupted.

To configure 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 group name Switch(config-red-aps)#	Specifies an APS group name and enters APS configuration mode. Note The group name is case sensitive.
Step 3	Switch(config-red-aps)# aps working wavepatch slot/subcard/port	Configures the working path interface.
Step 4	Switch(config-red-aps)# aps protection wavepatch slot/subcard/port	Configures the protection path interface.
Step 5	Switch(config-red-aps)# aps enable	Enables APS activity between the interfaces.

Examples

This example shows how to associate wavepatch interfaces for the transponder line card in slot 3 for splitter protection.

```
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
<code>show aps</code>	Displays the APS configuration summary.
<code>show aps {detail group name interface wavepatch slot/subcard/port}</code>	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, NA: Not Applicable
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
-----
Wavepatch8/0/0    Wk Ac Up LOL Wavepatch8/0/1          Seattle
Wavepatch8/0/1    Pr St Up -  Wavepatch8/0/0          Seattle

Switch# show aps group Seattle

APS Group Seattle :

architecture.: 1+1, remote prov: 1+1
span.....: end-to-end
prot. mode...: network side splitter
direction...: prov: uni, current: uni, remote prov: uni
revertive....: yes, wtr: 60 secs (not running)
aps state....: enabled (associated)
request timer: holddown: 5000 ms, max: 15000 ms, count 2
msg-channel...: auto (up on osc)
created.....: 0 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): 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
```

About Line Card Protection

Line card protection on the Cisco ONS 15530 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 15530 supports three types of line card protection:

- Client based protection
- Y-cable protection
- Switch fabric based protection

About Client Based Line Card Protection

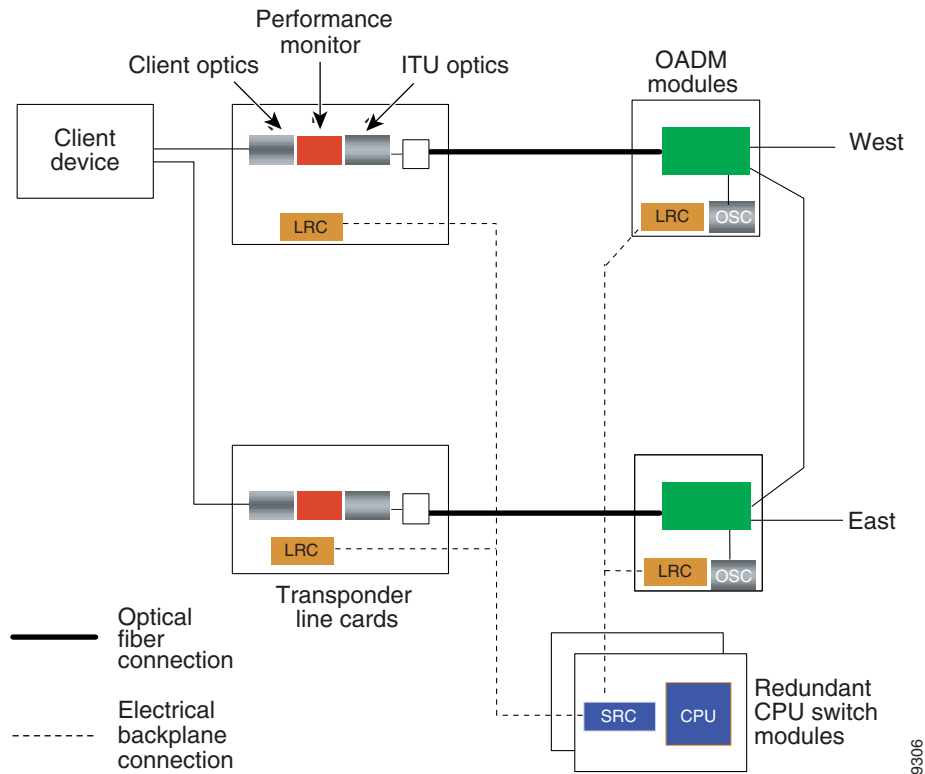
In client protection mode, both signals are transmitted to the client system. The client system decides which signal to use and when to switch over.

**Note**

Client protection does not require APS configuration on the Cisco ONS 15530.

Figure 10-3 shows an example of line card protection using transponder line cards.

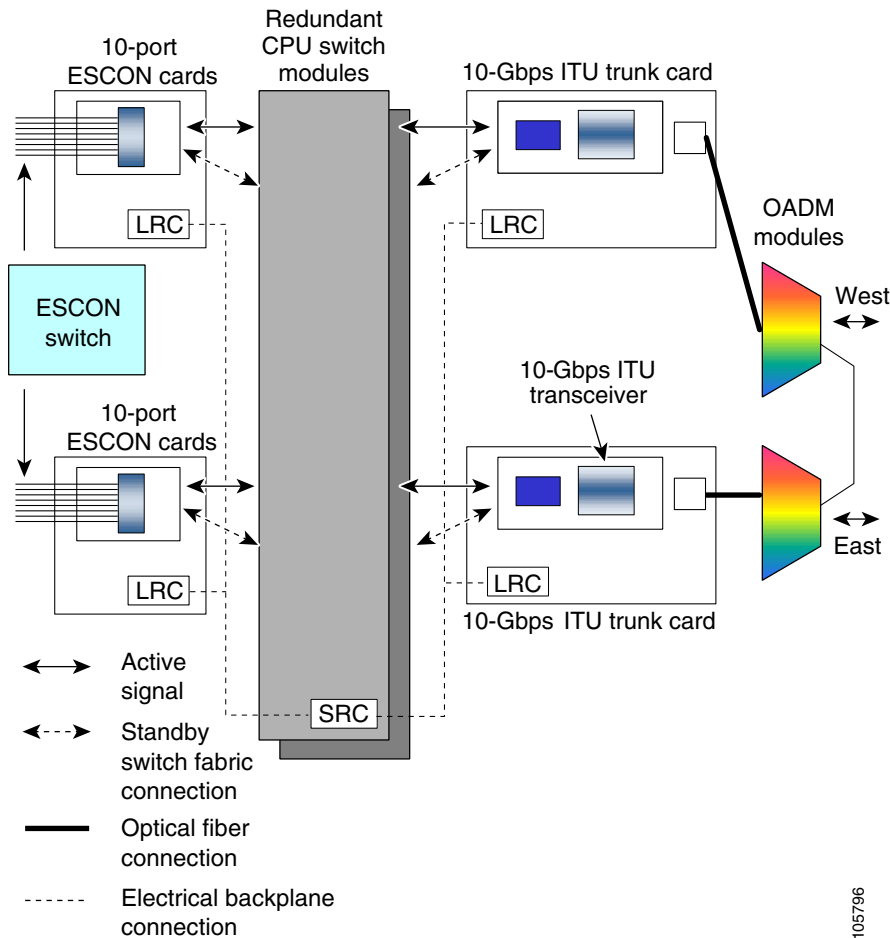
Figure 10-3 Client Based Line Card Protection Using Transponder Line Cards



79306

Figure 10-4 shows an example of line card protection using ESCON aggregation cards and 10-Gbps ITU trunk cards.

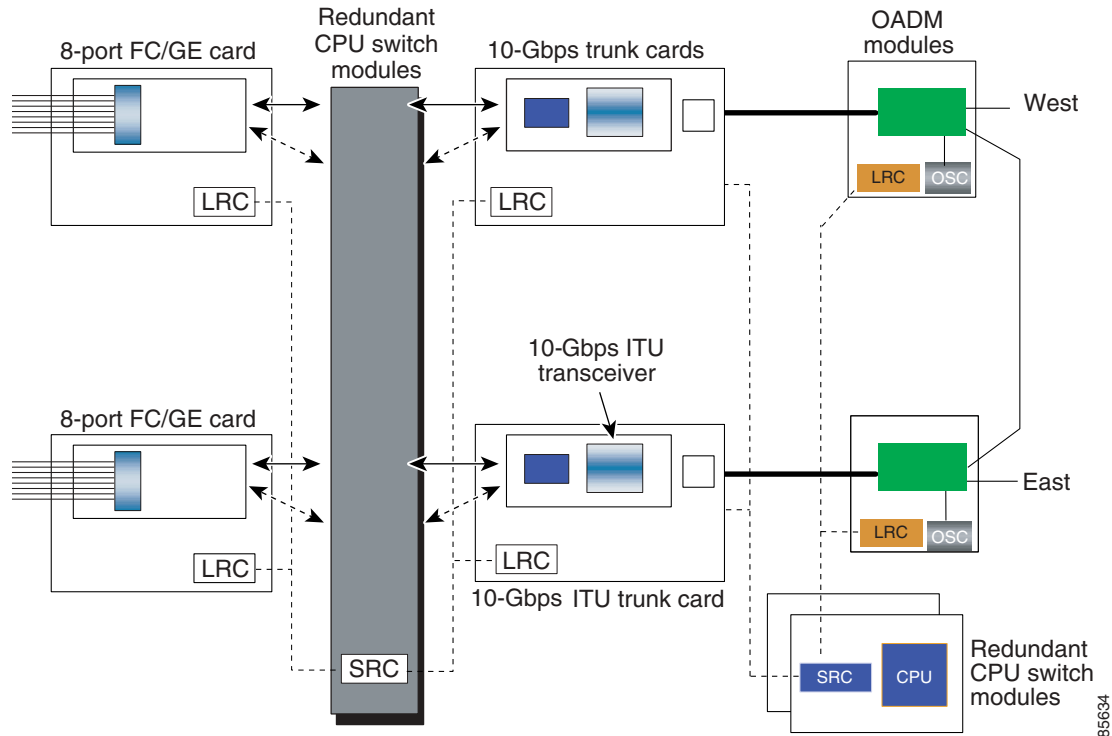
Figure 10-4 Client Based Line Card Protection Using ESCON Aggregation Cards and 10-Gbps ITU Trunk Cards



About Y-Cable Line Card Protection

With y-cable protection, the client equipment sends only one signal to two transponder line cards or two 8-port FC/GE aggregation cards using a y-cable to replicate the signal. The client equipment receives from only one line card. The Cisco ONS 15530 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 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 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. (See [Figure 10-5](#).)

Figure 10-5 Y-Cable Based Line Card Protection Scheme



85634

Considerations for Using Y-Cable Based Line Card Protection

The following considerations apply when considering the use of line card protection:

- 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 configuration can support up to 4 channels with line card protection using transponder line cards. A fully provisioned multiple shelf configuration can support up to 32 channels in line card protection mode.

For more information about multiple shelf nodes, see [Chapter 11, “Configuring Multiple 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 line cards that support the same channel. In this way the client signal maps to the same WDM wavelength on both the working and protection paths.



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 15530 Planning Guide](#).

Configuring Y-Cable Based Line Card Protection

The following is an overview of the tasks required to configure 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 OADM modules needed to support the deployed channels are installed in the shelf. (See the “[Considerations for Using Y-Cable Based Line Card Protection](#)” section on page 10-10.)
 - Step 3** Ensure that the OADM modules are correctly interconnected with the external optical patch cables.
 - Step 4** In order to ensure separate paths to the OADM modules, shut down the unused wavepatch interfaces if you are using splitter line cards.
 - 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 15530 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. Note The group name is case sensitive.
Step 3	Switch(config-red-aps)# aps working [transparent gigabitphy] <i>slot/subcard/port</i>	Configures the working path interface.
Step 4	Switch(config-red-aps)# aps protection [transparent gigabitphy] <i>slot/subcard/port</i>	Configures the protection path interface.
Step 5	Switch(config-red-aps)# aps y-cable	Enables y-cable protection. The default state is no y-cable protection (disabled).
Step 6	Switch(config-red-aps)# aps enable	Enables APS activity between the interfaces.



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.

```
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 4/0/0
Switch(config-red-aps)# aps y-cable
Switch(config-red-aps)# aps enable
Switch(config-red-aps)# end
Switch#
```

Displaying the Y-Cable Protection Configuration

To display the y-cable protection configuration, use the following EXEC command:

Command	Purpose
<code>show aps</code>	Displays the APS configuration summary.
<code>show aps {detail group name interface [transparent gigabitphy] slot/subcard/port}</code>	Displays detailed APS configuration information for interfaces and groups. Note Group names are case sensitive.

Example

The following example shows how to display the y-cable protection for an APS group:

```
Switch# show aps

AR : APS Role, Wk: Working, Pr: Protection
AS : APS State, Ac: Active, St: Standby, NA: Not Applicable
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
-----
Transparent4/0/0   Wk St Up -   Transparent7/0/0   Yosemite
Transparent7/0/0   Pr Ac Up SD  Transparent4/0/0   Yosemite

Switch# show aps group Yosemite

APS Group Yosemite :

architecture.: 1+1, remote prov: 1+1
span.....: end-to-end
prot. mode...: client side y-cable
direction....: prov: bi, current: bi, remote prov: bi
revertive....: no
aps state....: enabled (associated)
request timer: holddown: 5000 ms, max: 15000 ms, count 2
msg-channel...: auto (up on osc)
created.....: 17 hours, 10 minutes
auto-failover: enabled
transmit k1k2: reverse-request, 1, 1, 1+1, bi
receive k1k2: forced-switch, 1, 1, 1+1, bi
switched chan: 1
protection(0): Transparent7/0/0 (ACTIVE - UP), Wave7/0 (UP)
               : channel request: no-request
               : switchover count: 2
               : last switchover: 15 hours, 14 minutes
working...(1): Transparent4/0/0 (STANDBY - UP), Wave4/0 (UP)
               : channel request: no-request
```



```

: switchover count: 3
: last switchover: 14 hours, 41 minutes

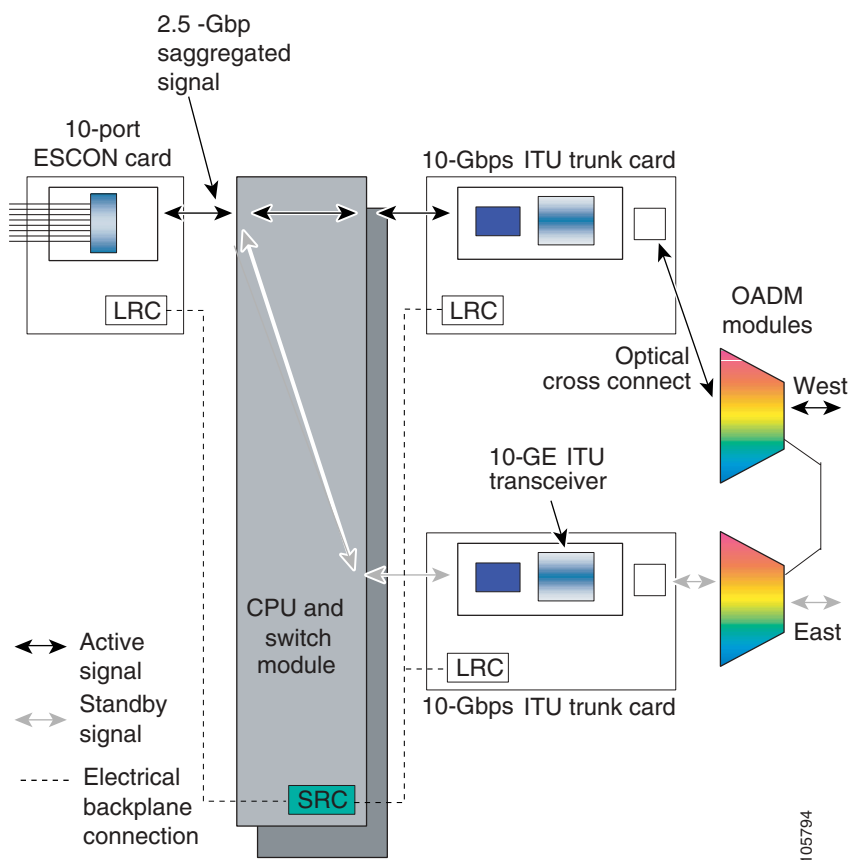
```

About Switch Fabric Based Line Card Protection

The Cisco ONS 15530 provides protection for cross connections through the switch fabric. Switch fabric based line card protection is supported on systems with one or two switch fabrics.

The aggregated signals from the aggregation cards cross connect through the switch fabric to a 2.5-Gbps ITU trunk card, 10-Gbps ITU trunk card, or 10-Gbps uplink card. In switch fabric based line card protection, the system sets up a protection cross connection through the switch fabric to a second 2.5-Gbps ITU trunk card, 10-Gbps ITU trunk card, or a 10-Gbps uplink card (see [Figure 10-6](#)).

Figure 10-6 Switch Fabric Based Line Card Protection with Redundant Switch Fabrics



Switch fabric based line card protection protects against facility failures and failures in 2.5-Gbps ITU trunk cards, 10-Gbps ITU trunk cards, and 10-Gbps uplink cards.



Note

Splitter protection and y-cable protection cannot be configured with switch fabric based protection.

Considerations for Using Switch Fabric Based Line Card Protection

The following considerations apply when considering the use of line card protection:

- Switch fabric based line card protection does not protect against failures of the client equipment or the ESCON aggregation card. To protect against such failures, use client based line card protection.
- A fully provisioned single shelf configuration can support up to two channels with switch fabric based line card protection. A fully provisioned multiple shelf configuration can support up to 32 channels in switch fabric based line card protection mode.

For more information about multiple shelf nodes, see [Chapter 11, “Configuring Multiple Shelf Nodes.”](#)


- Switch fabric based 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 line cards of the same channel. In this way the client signal maps to the same WDM wavelength on both the working and protection paths.
- Configure unique flow identifiers on the ESCON aggregation card interfaces. Duplicate flow identifiers interfere with switchovers between line cards.
- Be sure that the subinterface on the protection line card does not have a configured cross connection. Such cross connection interfere with switchovers.

Proper physical configuration of the system is critical to the operation of switch fabric based line card protection. For detailed information on shelf configuration rules, refer to the [Cisco ONS 15530 Planning Guide](#).

Configuring Switch Fabric Based Line Card Protection

To configure switch fabric based line card protection, use the following commands:

	Command	Purpose
Step 1	Switch# show connect	Displays the cross connect configuration.
Step 2	Switch# configure terminal Switch(config)#	Enters global configuration mode.
Step 3	Switch(config)# connect { waveethernetphy tengigethernetphy } <i>slot/subcard</i> [<i>subinterface</i>] portgroup <i>slot/subcard/port</i> [override]	Configures cross connections on the line card.
Step 4	Switch(config)# redundancy Switch(config-red)#	Enters redundancy configuration mode.
Step 5	Switch(config-red)# associate group <i>name</i> Switch(config-red-aps)#	Specifies an APS group name and enters APS configuration mode.
		Note The group name is case sensitive.

	Command	Purpose
Step 6	Switch(config-red-aps)# aps working { waveethernetphy tengigethernetphy } <i>slot/subcard</i>	Configures the working path interface.  Caution Configuring the working path on the standby cross connection might cause a switchover. Configure the working path on the active cross connection to prevent such switchovers when the APS group is enabled.
Step 7	Switch(config-red-aps)# aps protection { waveethernetphy tengigethernetphy } <i>slot/subcard</i>	Configures the protection path interface.
Step 8	Switch(config-red-aps)# aps enable	Enables APS activity between the interfaces.

**Note**

When configuring the esconphy interfaces, use unique flow identifiers for each esconphy interface on the system. For more information on configuring esconphy interfaces, see the [“Configuring ESCON Aggregation Card Interfaces”](#) section on page 4-3.

**Note**

You can configure cross connections on either the working or the protection 2.5-Gbps ITU trunk cards, 10-Gbps ITU trunk cards, or 10-Gbps uplink cards.

Displaying Switch Fabric Based Protection Configuration

To display the switch fabric based protection configuration, use the following EXEC command:

Command	Purpose
show aps [detail group <i>name</i> interface { waveethernetphy tengigethernetphy } <i>slot/subcard</i>]	Displays the APS configuration.

Example

The following example shows how to display the switch fabric based line card protection:

```
Switch# show aps detail
```

```
APS Group yellow :
```

```
architecture.: 1+1, remote prov: 1+1
span.....: end-to-end
prot. mode...: switch fabric based line card protection
direction...: prov: bi, current: bi, remote prov: bi
revertive....: no
aps state....: enabled (associated)
request timer: holddown: 5000 ms, max: 15000 ms, count 2
msg-channel..: auto-select (up on cdl dcc)
created.....: 0 minutes
auto-failover: enabled
transmit k1k2: no-request, 0, 0, 1+1, bi
receive k1k2: no-request, 0, 0, 1+1, bi
```

```

switched chan: 0
protection(0): WaveEthernetPhy8/0 (STANDBY - UP), xc DORMANT
                : channel request: no-request
                : switchover count: 0
                : last switchover: never
working...(1): WaveEthernetPhy7/0 (ACTIVE - UP), xc UP
                : channel request: no-request
                : switchover count: 0
                : last switchover: never

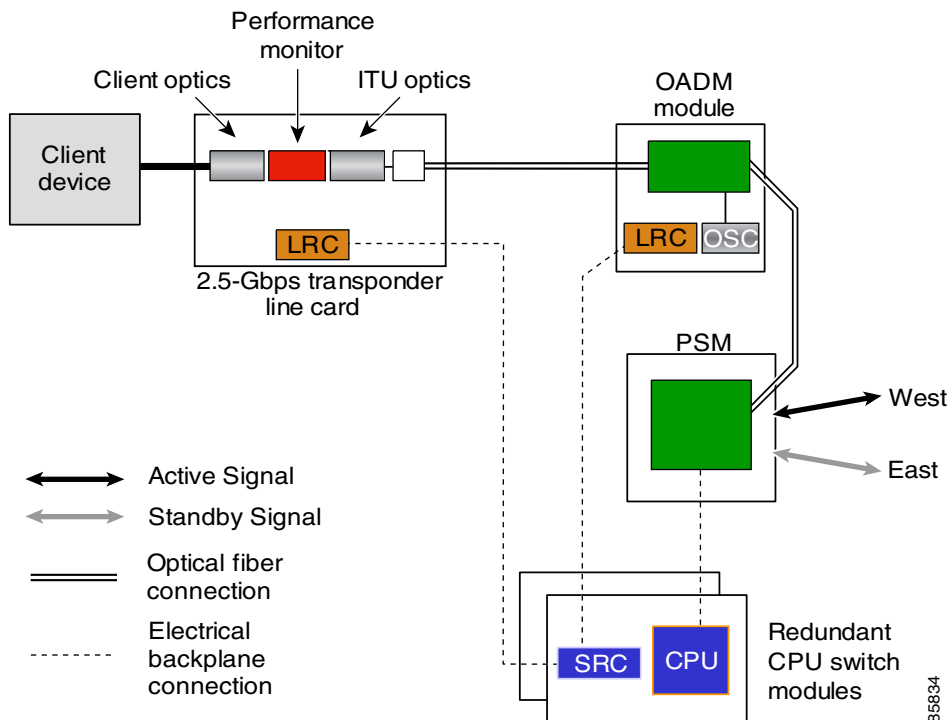
```

About Trunk Fiber Based Protection

The PSM (protection switch module) provides trunk fiber based protection for Cisco ONS 15530 systems configured in point-to-point topologies. This type of protection only provides protection against trunk fiber cuts, not specific channel failure as provided by splitter and line card based schemes. However, this protection scheme allows for much simpler shelf configurations in topologies where per channel protection is not required.

Figure 10-7 shows trunk fiber based protection configured with a transponder line card.

Figure 10-7 Trunk Fiber Based Protection With a Transponder Line Card



Considerations for Using Trunk Fiber Protection

The following considerations apply when using trunk fiber protection:

- Trunk fiber protection does not protect against failures on the shelf itself or the client equipment. To protect against these failures, line card protection should be implemented on the client equipment itself.
- The APS software that supports trunk fiber based protection can be configured as revertive or nonrevertive. After a switchover, the active traffic can be put back on the previously failed working fiber, once the fault has been remedied, either automatically (revertive) or through manual intervention (nonrevertive).
- Use PSMs only in point-to-point topologies.
- In multiple shelf nodes, the shelf connected to the trunk fiber must use a PSM.
- The point-to-point topology can have no more than two EDFAs. The cumulative noise of three or more EDFAs interferes with detecting the data channel loss on the PSM.
- When EDFAs are present in the topology, the power of the data channels at the PSM receiver must be greater than the cumulative noise of the EDFAs.
- Up to four channels on a single shelf can be protected with trunk fiber based protection.

Configuring Trunk Fiber Protection

To configure trunk fiber protection on the wdmsplit interfaces, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# redundancy Switch(config-red)#	Enters redundancy mode.
Step 2	Switch(config-red)# associate group name Switch(config-red-aps)#	Specifies an APS group name and enters APS configuration mode. Note The group name is case sensitive.
Step 3	Switch(config-red-aps)# aps working wdmsplit slot/subcard	Configures the working path interface.
Step 4	Switch(config-red-aps)# aps protection wdmsplit slot/subcard	Configures the protection path interface.
Step 5	Switch(config-red-aps)# aps message-channel {auto-select inband dcc ip osc} far-end name	Configures the name of the corresponding APS group on the other node in the topology.
Step 6	Switch(config-red-aps)# aps enable	Enables APS activity between the interfaces.

Examples

The following example shows how to configure trunk fiber protection:

```
Switch(config)# redundancy
Switch(config-red)# associate group psm-group
Switch(config-red-aps)# aps working wdmsplit 0/1/0
Switch(config-red-aps)# aps protection wdmsplit 0/1/1
Switch(config-red-aps)# aps message-channel auto-select far-end group-name psm-group
Switch(config-red-aps)# aps enable
```

Displaying Trunk Fiber Protection Configuration

To display the trunk fiber configuration, use the following EXEC command:

Command	Purpose
show aps [detail group name interface wdmsplit slot/subcard/port]	Displays the APS configuration for interfaces and groups.
	Note Group names are case sensitive.

Examples

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

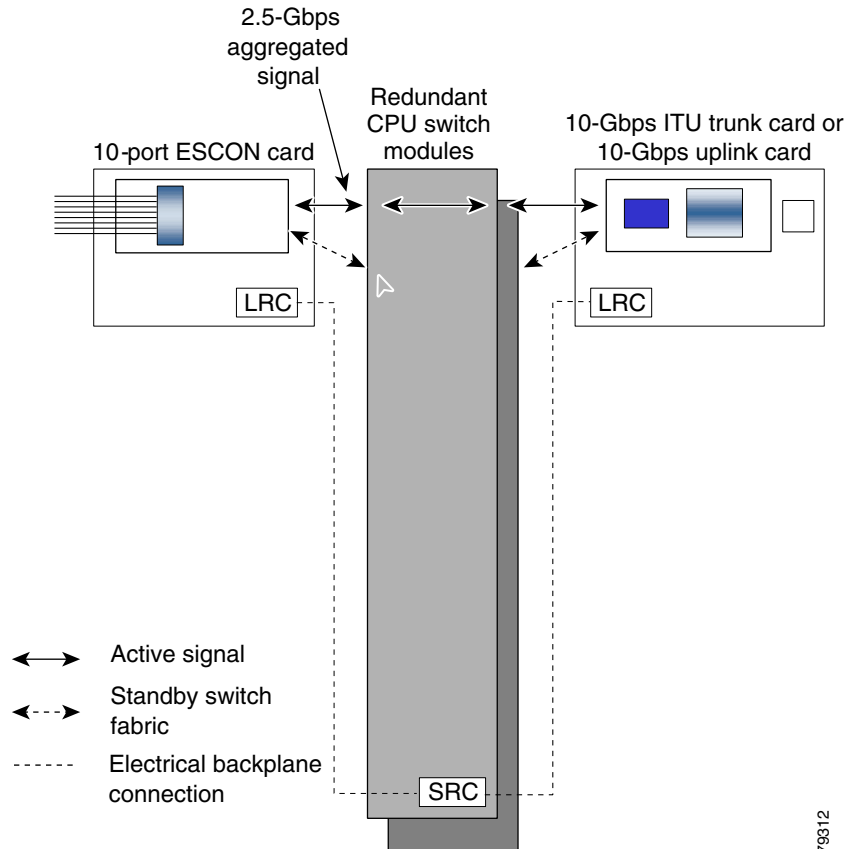
```
Switch# show aps group psm-group
APS Group psm-group :

architecture.:1+1, remote prov:uni
span.....:end-to-end
prot. mode...:network side wdm splitter
direction....:prov:uni, current:uni, remote prov:uni
revertive....:no
aps state....:enabled (associated)
request timer:holddown:5000 ms, max:15000 ms, count 2
msg-channel..:auto (down), psm-group
created.....:2 minutes
auto-failover:disabled
transmit k1k2:sf-lp, 0, 0, 1+1, uni
receive k1k2:no-request, 0, 0, unknown, unknown
switched chan:0
protection(0):WdmSplit0/0/1 (STANDBY - UP)
:channel request:sf-lp
:switchover count:1
:last switchover:0 minutes
working...(1):WdmSplit0/0/0 (ACTIVE - UP)
:channel request:sf-lp
:switchover count:1
:last switchover:0 minutes
```

About Redundant Switch Fabric Protection

The Cisco ONS 15530 provides protection for the 2.5-Gbps aggregated signals sent through the redundant switch fabrics. The switch fabrics connect signals from client side line cards, such as the ESCON aggregation card, to ITU side line cards, such as the 10-Gbps ITU trunk card (see [Figure 10-8](#)). When a shelf is configured for CPU switch module redundancy, the redundant switch fabric increases system availability by protecting against switch fabric failures.

Figure 10-8 Redundant Switch Fabrics



78312

Configuring APS Group Attributes

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

Configuring Revertive Switching

The Cisco ONS 15530 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.

	Command	Purpose
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 <i>seconds</i>	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 <i>name</i> interface { transparent <i>slot/subcard/0</i> wavepatch <i>slot/subcard/port</i> waveethernetphy <i>slot/subcard</i> gigabitphy <i>slot/subcard/port</i> wdmsplit <i>slot/subcard/port</i> }]	Displays the APS configuration for interfaces and groups. Note Group names are case sensitive.

Example

The following example shows how to display the 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 Unidirectional and Bidirectional Path Switching

The Cisco ONS 15530 supports per-channel unidirectional and bidirectional 1+1 path switching. When a signal is protected and the signal fails or degrades on the active path, the system automatically switches the APS group from the active network path to the standby network path.

Signal failures can be total LOL (loss of light) caused by laser failures, by fiber cuts between the Cisco ONS 15530 and the client equipment, between two Cisco ONS 15530s, or by other equipment failures. LOL failures on the transponder line cards and LOLK (loss of lock) on the 2.5-Gbps ITU trunk cards, 10-Gbps ITU trunk cards, and 10-Gbps uplink cards cause switchovers for protected signals.

For y-cable APS, you can also configure alarm thresholds to cause a switchover when the error rate detected on the signal reaches an unacceptable level. For information about configuring alarm thresholds, see the [“Configuring Alarm Thresholds” section on page 4-9](#).

The Cisco ONS 15530 implements path switching using an APS channel protocol over the in-band message channel, the OSC (optical supervisory channel), or the IP management connection.



Note

Bidirectional path switching operates only on networks that have the APS message channel configured over the OSC, the in-band message channel, or the IP management connection. You must configure the patch connection between the OSC module interfaces and the mux/demux module interface if you are using OSC for the APS message channel.

[Figure 10-9](#) 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 10-9 Active and Standby Path Configuration Example

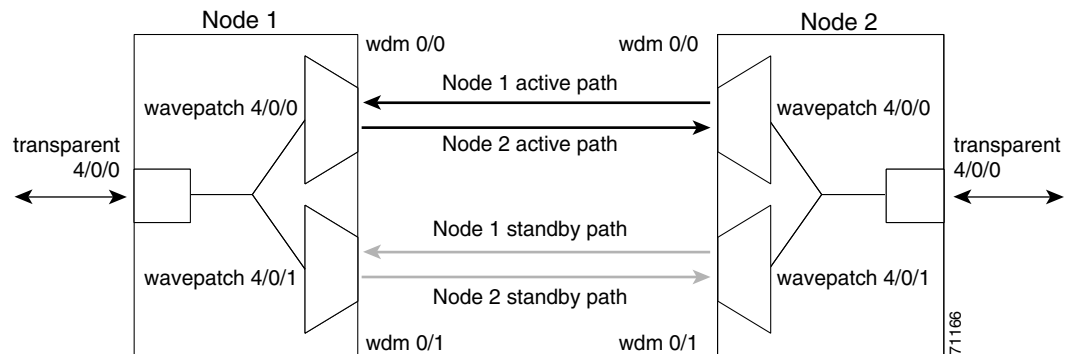


Figure 10-10 shows the behavior of unidirectional path switching when a loss of signal occurs. In the two node example network, unidirectional path switching operates as follows:

- Node 2 sends the 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 receive its original active path.

Now the nodes are communicating along different paths.

Figure 10-10 Unidirectional Path Switching Example

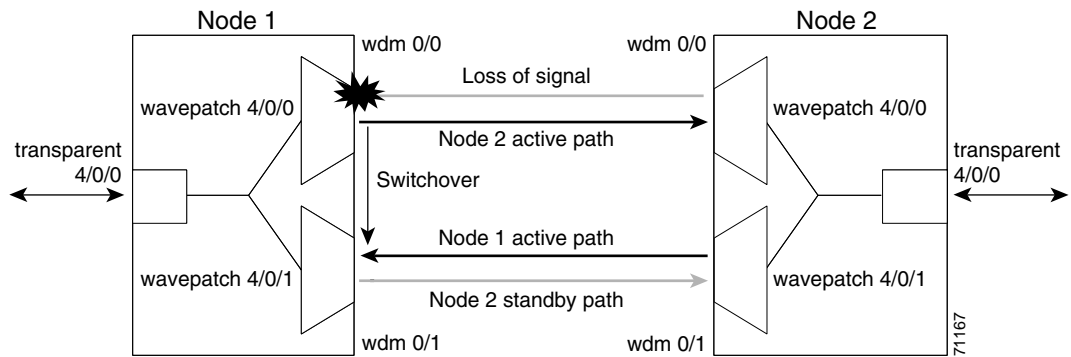
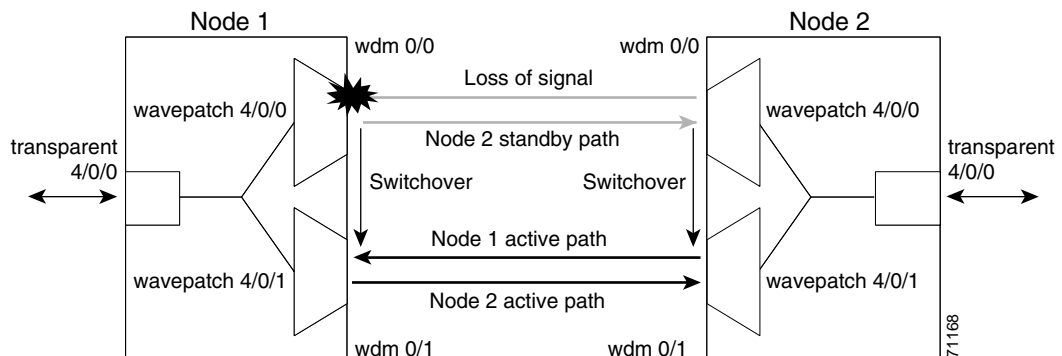


Figure 10-11 shows the behavior of bidirectional path switching when a loss of signal occurs. In the two node example network, bidirectional path switching operates as follows:

- Node 2 sends the 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 message to node 2 on the protection path indicating that it has switched.
- Node 2 processes the APS message and switches from the active path to the standby path.

Both node 1 and node 2 communicate on the same path.

Figure 10-11 Bidirectional Path Switching Overview



About APS Switching for Cisco ONS 15216 OADMs

The Cisco ONS 15530 can be connected to Cisco ONS 15216 OADMs in place of native Cisco ONS 15530 OADMs. However, this configuration does not support the Cisco ONS 15530 OSC channel (33rd channel, 1562.23 nm). For bidirectional path switching to function in this configuration, the APS message channel must operate through IP over the NME (Network Management Ethernet) on the CPU switch card. The Ethernet management ports of all the Cisco ONS 15530 and Cisco ONS 15216 systems at the site must connect to a single Ethernet switch, such as the Catalyst 2950, and must be managed over a single VLAN.

Configuring Unidirectional and Bidirectional 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.
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 timer message 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. (Optional)
Step 6	Switch(config-red-aps)# aps timer message max-interval seconds	Changes the APS Channel Protocol maximum interval timer for waiting for a message. The default is 15 seconds. (Optional) Repeat Step 1 through Step 6 on the corresponding transparent interface on the other node that adds and drops, or terminates, the channel.
Step 7	Switch(config-red-aps)# aps message-channel { auto-select [far-end group-name name] inband dcc [far-end group-name name] ip far-end group-name name ip-address ip-address osc [far-end group-name name]} Note For node configurations using Cisco ONS 15216 OADMs exclusively, use ip for the APS message channel.	Configures the message channel for the APS channel protocol messages. The default is auto-select without a group name. (Optional) Note For node configurations using Cisco ONS 15216 OADMs exclusively, use ip for the APS message channel.
Step 8	Switch(config-red-aps)# aps revertive	Configures revertive path switching. Default is nonrevertive.
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.

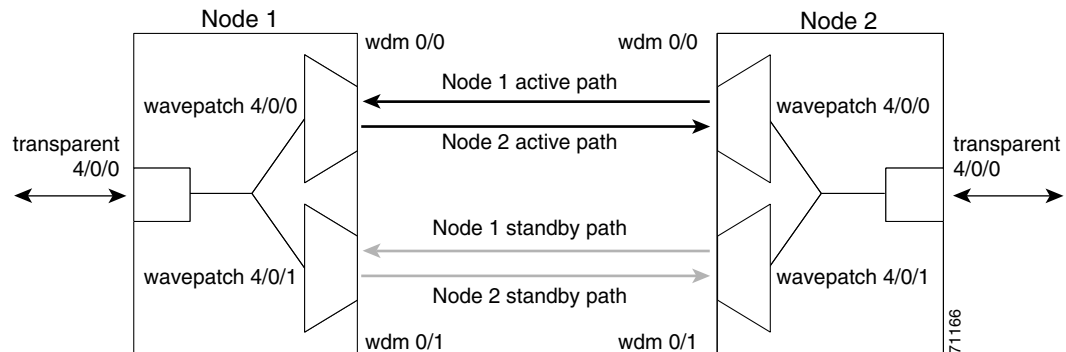
**Note**

For interfaces with either Sysplex ETR or Sysplex CLO protocol encapsulation, configure bidirectional path switching to ensure proper functioning of the protocol.

Examples

Figure 10-12 shows the active and standby paths between two Cisco ONS 15530 nodes, node 1 and node 2, with splitter protection.

Figure 10-12 Bidirectional Path Switching Example with Splitter Protection



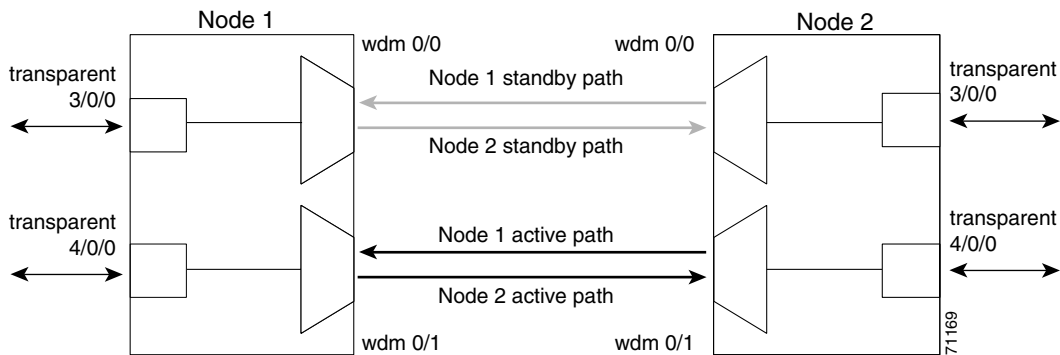
The following example shows how to configure one channel in the example network for bidirectional path switching using the default working and protection path interfaces:

```
Node1# configure terminal
Node1(config)# redundancy
Node1(config-red)# associate group red
Node1(config-red-aps)# aps working wavepatch 4/0/0
Node1(config-red-aps)# aps protection wavepatch 4/0/1
Node1(config-red-aps)# aps direction bidirectional
Node1(config-red-aps)# aps enable

Node2# configure terminal
Node2(config)# redundancy
Node2(config-red)# associate group red
Node2(config-red-aps)# aps working wavepatch 4/0/0
Node2(config-red-aps)# aps protection wavepatch 4/0/1
Node2(config-red-aps)# aps bidirectional
Node2(config-red-aps)# aps enable
```

Figure 10-13 shows the active and standby paths between two Cisco ONS 15530 nodes, node 1 and node 2 with y-cable protection.

Figure 10-13 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:

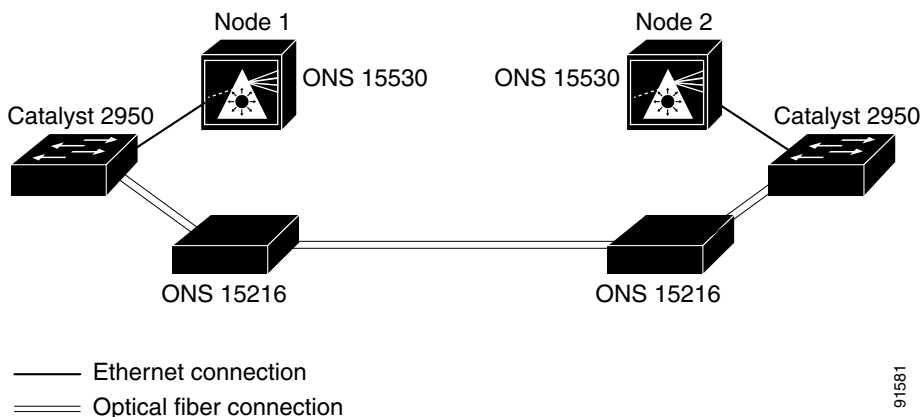
```

Node1# configure terminal
Node1(config)# redundancy
Node1(config-red)# associate group alpha
Node1(config-red-aps)# aps working transparent 4/0/0
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 4/0/0
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
    
```

Figure 10-14 shows the configuration two Cisco ONS 15530 nodes, node 1 and node 2, using Cisco ONS 15216 OADMs and the NME to manage the APS switchovers.

Figure 10-14 Bidirectional Path Switching Example with Cisco ONS 15216 OADMs



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

```

Node1# configure terminal
Node1(config)# interface fastethernet 0
Node1(config-if)# ip address 172.16.22.125 255.255.255.0
Node1(config-if)# no shutdown
Node1(config-if)# exit
Node1(config)# redundancy
Node1(config-red)# associate group one
Node1(config-red-aps)# aps working transparent 4/0/0
Node1(config-red-aps)# aps protection transparent 3/0/0
Node1(config-red-aps)# aps direction bidirectional
Node1(config-red-aps)# aps revertive
Node1(config-red-aps)# aps message-channel far-end group-name one ip-address 172.16.22.126
Node1(config-red-aps)# aps y-cable
Node1(config-red-aps)# aps enable
Node1(config-red-aps)# exit
Node1#

Cat2950-1# configure terminal
Cat2950-1(config)# interface gigabitethernet 0/1
Cat2950-1(config-if)# channel-group 1 mode on
Cat2950-1(config-if)# exit
Cat2950-1(config)# interface gigabitethernet 0/2
Cat2950-1(config-if)# channel-group 1 mode on
Cat2950-1(config-if)# exit
Cat2950-1(config)# interface vlan1
Cat2950-1(config-if)# ip address 10.0.0.1 255.255.255.0
Cat2950-1(config-if)# end
Cat2950-1#

Node2# configure terminal
Node2(config)# interface fastethernet 0
Node2(config-if)# ip address 172.16.22.126 255.255.255.0
Node2(config-if)# no shutdown
Node2(config-if)# exit
Node2(config)# redundancy
Node2(config-red)# associate group one
Node2(config-red-aps)# aps working transparent 4/0/0
Node2(config-red-aps)# aps protection transparent 3/0/0
Node2(config-red-aps)# aps direction bidirectional
Node2(config-red-aps)# aps revertive
Node2(config-red-aps)# aps message-channel far-end group-name one ip-address 172.16.22.125
Node2(config-red-aps)# aps y-cable
Node2(config-red-aps)# aps enable
Node2(config-red-aps)# exit
Node2#

Cat2950-2# configure terminal
Cat2950-2(config)# interface gigabitethernet 0/1
Cat2950-2(config-if)# channel-group 1 mode on
Cat2950-2(config-if)# exit
Cat2950-2(config)# interface gigabitethernet 0/2
Cat2950-2(config-if)# channel-group 1 mode on
Cat2950-2(config-if)# exit
Cat2950-2(config)# interface vlan1
Cat2950-2(config-if)# ip address 10.0.0.3 255.255.255.0
Cat2950-2(config-if)# end
Cat2950-2#

```

Displaying the Unidirectional and Bidirectional Path Switching Configuration

To display the path switching configuration, use the following EXEC command:

Command	Purpose
show aps [detail group <i>name</i> interface { transparent <i>slot/subcard/0</i> wavepatch <i>slot/subcard/port</i> waveethernetphy <i>slot/subcard/0</i> gigabitphy <i>slot/subcard/port</i> wdmsplit <i>slot/subcard/port</i> }]	Displays the APS configuration for interfaces and groups. Note Group names are case sensitive.

Example

The following example shows how to display the 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
→ msg-channel..: auto (up on osc)
  created.....: 26 minutes
  aps state....: associated
→ request timer: holddown: 5000 ms, max: 15 secs, count 2
  transmit k1k2: reverse-request, 1, 1, 1+1, bi
  receive k1k2: forced-switch, 1, 1, 1+1, bi
  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 15530 prevents any automatic switchover from the protection path to the working path until it has expired. When it expires, switchovers occur only if there is no fault on the working path and there is no overriding switchover request in effect.

To configure the switchover-enable timer, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# redundancy Switch(config-red)#	Enters redundancy configuration mode.
Step 2	Switch(config-red)# associate group <i>name</i> Switch(config-red-aps)#	Selects the interfaces to associate and enters APS configuration mode. Note The group name is case sensitive.
Step 3	Switch(config-red-aps)# aps disable	Disables the APS group.
Step 4	Switch(config-red-aps)# aps timer switchover-enable min-interval <i>seconds</i>	Modifies the timer that controls the check on the status of the working path. The default is 3 seconds.
Step 5	Switch(config-red-aps)# aps enable	Enables the APS group.

Displaying the Switchover-Enable Timer Configuration

To display the switchover-enable timer configuration, use the following EXEC command:

Command	Purpose
show aps [<i>detail</i> group <i>name</i> interface { <i>transparent slot/subcard/0</i> wavepatch <i>slot/subcard/port</i> waveethernetphy <i>slot/subcard</i> gigabitphy <i>slot/subcard/port</i> wdmsplit <i>slot/subcard/port</i> }]	Displays the APS configuration for interfaces and groups. Note Group names are case sensitive.

Example

The following example shows how to display the 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....: yes
  msg-channel..: auto (up on osc)
  created.....: 26 minutes
  aps state....: associated
  request timer: holddown: 5000 ms, max: 15 secs, count 2
  transmit k1k2: reverse-request, 1, 1, 1+1, bi
  receive k1k2: forced-switch, 1, 1, 1+1, bi
  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
```


About 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. 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 repairing the protection path when it degrades or fails.

The Cisco ONS 15530 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 are only honored if there is no lockout, forced switchover, or signal failure or degrade.

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 protection path
6. Signal degrade on the working path
7. Manual switchover

If a request or condition of a higher priority is in effect, a lower priority request is rejected.

**Note**

APS lockouts and forced or manual switchover requests 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 <i>group-name</i>	Locks out all switchovers to the protection path.
aps switch <i>group-name</i> { 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 blue
```

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 waveethernetphy <i>slot/subcard</i> wdmsplit slot/subcard/port }]	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 blue
```

```
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: uni
revertive....: no
msg-channel...: auto (up on osc)
created.....: 15 hours, 1 minute
aps state....: associated (enabled)
request timer: holddown: 5000 ms, max: 15000 ms, count 2
transmit k1k2: reverse-request, 1, 1, 1+1, bi
receive k1k2: forced-switch, 1, 1, 1+1, bi
switched chan: 0
```

```

→ channel ( 0): Transparent4/0/0 (STANDBY - UP), Wave4/0 (UP)
→       : channel request: lockout-of-protection
       : transmit request: lockout-of-protection
       : receive request: no-request
channel ( 1): Transparent2/0/0 (ACTIVE - UP), Wave2/0 (UP)
       : channel request: no-request
       : switchover count: 0
       : last switchover: never

```

Clearing Switchovers and Lockouts

A lockout stays in effect until the system reboots. A forced or manual switchover request stays in effect until the system reboots or a higher priority request preempts it. You can manually clear these requests from the CLI.

To clear an APS switchover or lockout request, use the following privileged EXEC command:

Command	Purpose
aps clear <i>group-name</i>	Clears APS switch request or lockout on an associated interface pair.

Example

The following example shows how to clear the requests on an associated interface pair using the default group name:

```
Switch# aps clear blue
```

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 waveethernetphy slot/subcard gigethernetphy slot/subcard }]	Displays the APS configuration for interfaces and groups. Note Group names are case sensitive.

The following example shows how to display the lockout and switchover request 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: uni
revertive....: no
msg-channel..: auto (up on osc)
created.....: 15 hours, 1 minute
aps state....: associated (enabled)
request timer: holddown: 5000 ms, max: 15000 ms, count 2
transmit k1k2: reverse-request, 1, 1, 1+1, bi
receive k1k2: forced-switch, 1, 1, 1+1, bi

```

```
switched chan: 0
channel ( 0): Transparent4/0/0 (STANDBY - UP), Wave4/0 (UP)
→          : channel request: lockout-of-protection
→          : transmit request: lockout-of-protection
           : receive request: no-request
channel ( 1): Transparent2/0/0 (ACTIVE - UP), Wave2/0 (UP)
           : channel request: no-request
           : switchover count: 0
           : last switchover: never
```



Configuring Multiple Shelf Nodes

This chapter describes how to configure a multiple shelf node in a network topology. This chapter contains the following sections:

- [About Multiple Shelf Nodes, page 11-1](#)
- [Configuring Multiple Shelf Nodes, page 11-1](#)

About Multiple Shelf Nodes

On a single Cisco ONS 15530 shelf, only 4 channels can be supported. By cascading multiple Cisco ONS 15530 shelves, up to 32 channels can be supported. You can use multiple 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 Multiple Shelf Nodes

To configure a multiple shelf node, follow these steps:

-
- Step 1** Populate the shelves with the motherboards, cards, and processor cards.
 - Step 2** Connect the OADM modules with cables and configure the patch connections.
 - Step 3** Configure the client interfaces.
 - Step 4** 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 5** Configure IP addresses on the OSC wave interfaces.
For information on configuring an IP address on the OSC wave interface, see the [“Configuring IP on the OSC” section on page 12-8](#).
 - Step 6** Configure the network topology information for the connections between the two shelves.
 - Step 7** Configure APS (Automatic Protection Switching) on the shelves in the network that support the channels.
-

Configuring Patch Connections Between Shelves

To represent the three shelves as one node in the network topology, you must configure the patch connection between the shelves in the CLI (command-line interface). To configure these connections, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch1(config)# interface { <i>wave slot</i> <i>oscard slot/subcard</i> <i>thru slot/subcard</i> <i>wdm slot/subcard</i> }	Selects the interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# topology neighbor { <i>name node-name</i> ip-address <i>node-ip-address</i> mac-address <i>node-mac-address</i> } { port { <i>name port-name</i> ip-address <i>port-ip-address</i> mac-address <i>port-mac-address</i> }}	Configures the network topology information for a neighboring node.
Step 3	Switch(config-if)# topology neighbor agent ip-address <i>ip-address</i>	Specifies the address of the network topology agent on a neighboring node.

Examples

The following example shows how to configure the patch connections between the OADM modules on the three shelves in the example node:

```
Shelf1(config)# interface wdm 0/0
Shelf1(config-if)# topology neighbor name node1 port name wdm 0/1
Shelf1(config-if)# topology neighbor agent ip-address 10.1.1.1
Shelf1(config-if)# exit
Shelf1(config)# interface thru 0/0
Shelf1(config-if)# topology neighbor name shelf2 port name wdm 0/0
Shelf1(config-if)# topology neighbor agent ip-address 10.2.2.2
Shelf1(config-if)# exit
Shelf1(config)# interface wdm 0/1
Shelf1(config-if)# topology neighbor name shelf2 port name thru 0/1
Shelf1(config-if)# topology neighbor agent ip-address 10.2.2.2
Shelf1(config-if)# exit
Shelf1(config)# interface thru 0/1
Shelf1(config-if)# topology neighbor name shelf3 port name thru 0/0
Shelf1(config-if)# topology neighbor agent ip-address 10.2.2.3
Shelf1(config-if)# exit

Shelf2(config)# interface wdm 0/0
Shelf2(config-if)# topology neighbor name shelf1 port name thru 0/0
Shelf2(config-if)# topology neighbor agent ip-address 10.2.2.1
Shelf2(config-if)# exit
Shelf2(config)# interface thru 0/0
Shelf2(config-if)# topology neighbor name shelf3 port name wdm 0/0
Shelf2(config-if)# topology neighbor agent ip-address 10.2.2.3
Shelf2(config-if)# exit
Shelf2(config)# interface wdm 0/1
Shelf2(config-if)# topology neighbor name shelf3 port name thru 0/1
Shelf2(config-if)# topology neighbor agent ip-address 10.2.2.3
Shelf2(config-if)# exit
Shelf2(config)# interface thru 0/1
Shelf2(config-if)# topology neighbor name shelf1 port name wdm 0/1
Shelf2(config-if)# topology neighbor agent ip-address 10.2.2.1
Shelf2(config-if)# exit
```

```

Shelf3(config)# interface wdm 0/0
Shelf3(config-if)# topology neighbor name Shelf2 port name thru 0/0
Shelf3(config-if)# topology neighbor agent ip-address 10.2.2.2
Shelf3(config-if)# exit
Shelf3(config)# interface thru 0/0
Shelf3(config-if)# topology neighbor name shelf1 port name thru 0/1
Shelf3(config-if)# topology neighbor agent ip-address 10.2.2.1
Shelf3(config-if)# exit
Shelf3(config)# interface wdm 0/1
Shelf3(config-if)# topology neighbor name Node3 port name thru 0/0
Shelf3(config-if)# topology neighbor agent ip-address 10.3.3.1
Shelf3(config-if)# exit
Shelf3(config)# interface thru 0/1
Shelf3(config-if)# topology neighbor name shelf2 port name wdm 0/1
Shelf3(config-if)# topology neighbor agent ip-address 10.2.2.2
Shelf3(config-if)# exit

```

Configuring APS

When a multiple shelf node is part of a network topology, the channels supported by it might require special configuration. On a multiple shelf node, the OSC might have only one connection or no OSC connections at all. 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 multiple shelf node without full OSC support, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch1(config)# redundancy Switch1(config-red)#	Enters redundancy configuration mode.
Step 2	Switch(config-red)# associate group <i>name</i> Switch(config-red-aps)#	Specifies an APS group name and enters APS configuration mode. Note The group name is case sensitive.
Step 3	Switch(config-red-aps)# aps disable	Disables APS activity between the interfaces. Note For newly created APS groups, APS activity is disabled by default.
Step 4	Switch(config-red-aps)# aps working wavepatch <i>slot/subcard/port</i>	Configures the working path interface.
Step 5	Switch(config-red-aps)# aps protection wavepatch <i>slot/subcard/port</i>	Configures the protection path interface.
Step 6	Switch1(config-red-aps)# aps y-cable	Enables y-cable protection. The default state is no y-cable protection (disabled).
Step 7	Switch1(config-red-aps)# aps message-channel ip far-end group <i>group-name ip-address address</i>	Configures the APS group name and IP address on the remote node that supports the channel.
Step 8	Switch1(config-red-aps)# aps enable	Enables APS activity between the interfaces.

For more information on configuring y-cable line card protection, refer to the “[Configuring Y-Cable Based Line Card Protection](#)” section on page 10-11.

Examples

For these examples, assume the following:

- Channels 17-20 terminate on the second shelf of the multiple shelf node.
- The second shelf of the multiple shelf node has no OSC support.
- The management IP address of the second shelf of the multiple 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 1/0/0
Switch(config-red-aps)# aps protection transparent 2/0/0
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 3/0/0
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 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 7/0/0
Switch(config-red-aps)# aps protection transparent 8/0/0
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 9/0/0
Switch(config-red-aps)# aps protection transparent 10/0/0
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 through 20 on shelf 3 of a multiple shelf node.

```
Shelf3(config)# redundancy
Shelf3(config-red)# associate group Channel17
Shelf3(config-red-aps)# aps working transparent 1/0/0
Shelf3(config-red-aps)# aps protection transparent 2/0/0
Shelf3(config-red-aps)# aps y-cable
Shelf3(config-red-aps)# aps far-end group Channel17 ip-address 10.3.2.1
Shelf3(config-red-aps)# aps enable
Shelf3(config-red-aps)# exit
Shelf3(config-red)# associate group Channel18
Shelf3(config-red-aps)# aps working transparent 3/0/0
Shelf3(config-red-aps)# aps protection transparent 4/0/0
Shelf3(config-red-aps)# aps y-cable
Shelf3(config-red-aps)# aps far-end group Channel18 ip-address 10.3.2.1
Shelf3(config-red-aps)# aps enable
Shelf3(config-red-aps)# exit
Shelf3(config-red)# associate group Channel19
Shelf3(config-red-aps)# aps working transparent 7/0/0
```



```
Shelf3(config-red-aps)# aps protection transparent 8/0/0
Shelf3(config-red-aps)# aps y-cable
Shelf3(config-red-aps)# aps far-end group Channel19 ip-address 10.3.2.1
Shelf3(config-red-aps)# aps enable
Shelf3(config-red-aps)# exit
Shelf3(config-red)# associate group Channel20
Shelf3(config-red-aps)# aps working transparent 9/0/0
Shelf3(config-red-aps)# aps protection transparent 10/0/0
Shelf3(config-red-aps)# aps y-cable
Shelf3(config-red-aps)# aps far-end group Channel20 ip-address 10.3.2.1
Shelf3(config-red-aps)# aps enable
Shelf3(config-red-aps)# end

Shelf3# copy system:running-config nvram:startup-config
```




Monitoring Your Network Topology

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

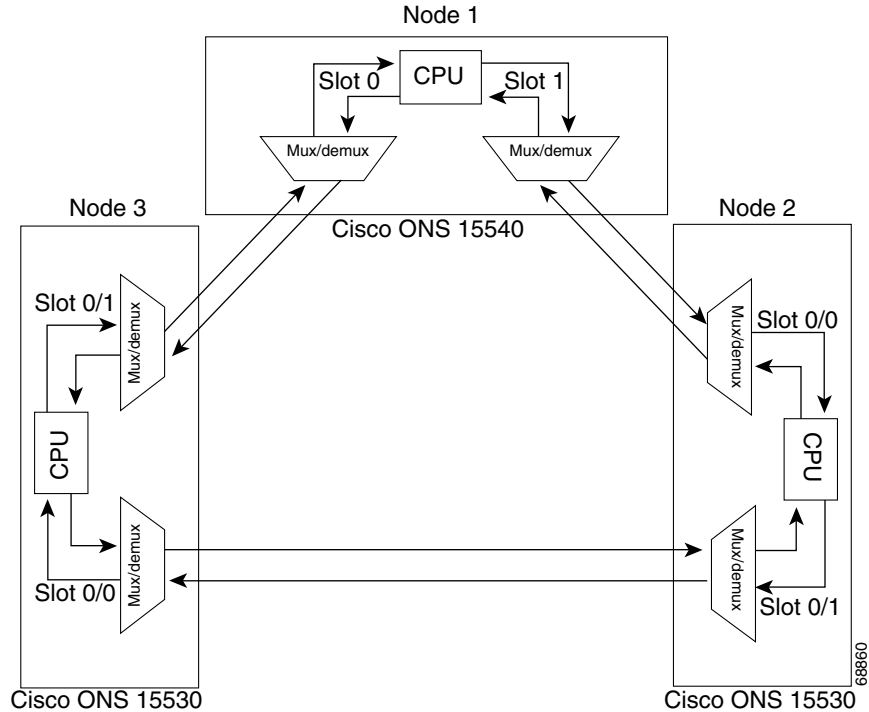
- [About the OSC, page 12-1](#)
- [Configuring CDP, page 12-3](#)
- [Configuring OSCP, page 12-6](#)
- [Configuring IP on the OSC, page 12-8](#)
- [Configuring IP on Ethernetdce Interfaces for the In-Band Message Channel, page 12-12](#)
- [Configuring SNMP, page 12-15](#)
- [Monitoring Without the OSC or In-Band Message Channel, page 12-19](#)
- [Configuring Interfaces in the Network Topology, page 12-21](#)
- [About Embedded CiscoView, page 12-22](#)
- [Installing and Configuring Embedded CiscoView, page 12-22](#)

About the OSC

As described in the [“OSC Modules” section on page 1-8](#), the Cisco ONS 15530 dedicates a separate channel (channel 0) for the OSC (optical supervisory channel), which is used for network control and management information between Cisco ONS 15530 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 12-1](#) shows the path of the OSC in a protected ring configuration. The OSC signal is generated by a laser on an OSC card 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 12-1 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 15530 network with a single Ethernet connection. Also, just one Ethernet connection is required from the NMS to monitor all Cisco ONS 15530 systems on the network using SNMP.

Hardware Guidelines for Using OSC

To provide protection against failure of the laser or a fiber break in protected configurations (point-to-point or ring), the following rules apply:

- One slot contains a carrier motherboard with two OSC cards.
- Both OADM modules must support OSC along with the band of wavelengths.

For more information on hardware configuration rules, refer to the *Cisco ONS 15530 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 15530, you can configure CDP at both the global level and the interface level. The global-level CDP configuration sets the attributes for the entire system. The interface-level configuration identifies interfaces connected to the client equipment and to the trunk interface to CDP. Because there are only optical connections to the client equipment, you must explicitly identify the transparent interfaces connected to the client equipment. On wdm interfaces, you can choose to provide the information about the interface in the CLI or you can let CDP discover it.



Note

The shelf must include the OSC to support CDP. If the OSC is not present, see the “[Monitoring Without the OSC or In-Band Message Channel](#)” section on page 12-19.

Configuring Global CDP

To configure CDP on your Cisco ONS 15530, use the following commands in global configuration mode:

Command	Purpose
<code>cdp advertise-v2</code>	Specifies CDP version 2 advertisements. The default is version 2.
<code>cdp holdtime seconds</code>	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.
<code>cdp timer seconds</code>	Specifies how often to send CDP updates. The default value is 60 seconds.
<code>[no] cdp run</code>	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
<code>show cdp</code>	Displays the configured CDP timer, holdtime, and advertisement settings.

Example

The following example shows how to display the configured CDP values:

```
Switch> show cdp
Global CDP information:
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 180 seconds
  Sending CDPv2 advertisements is enabled
```

Displaying Global CDP Information

You can display information gathered by CDP, including a specific neighbor device listed in the CDP table, the interfaces on which CDP is enabled, and the traffic between devices gathered using CDP.

To display the CDP information, use the following EXEC commands:

Command	Purpose
show cdp entry [* <i>entry-name</i>] [protocol version]	Displays information about all neighbors or a specific neighbor discovered by CDP. Optionally, displays the protocol and version.
show cdp interface [<i>type number</i>]	Displays information about the interfaces on which CDP is enabled.
show cdp neighbors	Displays a list of CDP neighbors.
show cdp traffic	Displays information about traffic between devices gathered using CDP.

Example

The following example shows how to display CDP status and activity information:

```
Switch1# show cdp entry *
-----
Device ID: Switch2
Entry address(es):
  IP address: 10.1.1.2
Platform: cisco , Capabilities: Router
Interface: Wave2/0, Port ID (outgoing port): Wave2/0
Holdtime : 176 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) ONS-15530 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
Wave2/0 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        Wave2/0         158        R           Wave2/0   Wave2/0
```

```
Switch1# show cdp traffic
CDP counters :
  Total packets output: 18, Input: 20
  Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
  No memory: 0, Invalid packet: 0, Fragmented: 0
  CDP version 1 advertisements output: 0, Input: 0
  CDP version 2 advertisements output: 18, Input: 20
```

Clearing Global CDP Information

You can reset the CDP traffic counters to zero and clear the table that contains the CDP neighbor information. To clear the CDP information, use the following privileged EXEC commands:

Command	Purpose
<code>clear cdp counters</code>	Resets the CDP traffic counters to zero.
<code>clear cdp table</code>	Clears the table that contains the CDP neighbor information.

Configuring CDP Topology Discovery on Wdm 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 15530 enables CDP topology discovery by default on the wdm interfaces connecting to the trunk fiber.



Note

When a patch connection between an OADM module and a PSM is configured, topology learning on the wdm interface is disabled.

To configure CDP topology discovery on wdm interfaces, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# topology hold-time <i>seconds</i>	Modifies the interval to hold a nonstatic network topology node entry. The default value is 300 seconds.
Step 2	Switch(config)# interface <i>wdm slot/subcard</i> Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 3	Switch(config-if)# topology neighbor cdp [proxy interface] 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 discovery 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
<code>show topology neighbor [detail]</code>	Displays information about the physical network topology neighbors for the node.
<code>show topology</code>	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
Trans8/0/0	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
ospf timer hello interval <i>milliseconds</i>	Configures the Hello interval timer in milliseconds. The default value is 3000 milliseconds.

Example

The following example shows how to set the Hello interval to 500 milliseconds:

```
Switch(config)# ospf timer hello interval 500
```

Configuring the Hello Hold-Down Timer

The Hello hold-down timer specifies the interval during which no more than one Hello packet can be sent. If more than one Hello packet is generated during the hold-down period, the extra packets are delayed. Increasing the hold-down timer limits the number of Hello packets triggered in response to Hello packets received from a neighboring node and reduces the likelihood of Hello packets flooding the OSC.

To configure the OSCP Hello hold-down timer, use the following global configuration command:

Command	Purpose
ospf timer hello holddown <i>milliseconds</i>	Configures the Hello hold-down timer in milliseconds. The default value is 100 milliseconds.

Example

The following example shows how to set the Hello hold-down timer to 2000 milliseconds:

```
Switch(config)# ospf timer hello holddown 2000
```

Configuring the Inactivity Factor

The OSCP inactivity factor determines whether or not to declare a link down. The inactivity factor is multiplied by the advertised Hello timer interval of the other node to produce the inactivity time interval. If the system does not receive OSCP packets from the other node before the expiration of the inactivity time interval, the link is declared down.

To configure the OSCP inactivity factor, use the following global configuration command:

Command	Purpose
ospf timer inactivity-factor <i>factor</i>	Configures inactivity factor as a multiple of the Hello interval. The default multiplier is 5.

Example

The following example shows how to configure the inactivity factor to 10 times the Hello interval value:

```
Switch(config)# ospf timer inactivity-factor 10
```

Displaying the OSCP Configuration

You can display the OSCP version, node ID, interfaces, and configured protocol parameters. To display the OSCP configuration, use the following EXEC command:

Command	Purpose
<code>show oscp info</code>	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
<code>show oscp neighbor</code>	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
  ~~~~~
Wave7/0       20E0000   20E0000     2way
```

Configuring IP on the OSC

Configuring IP on the OSC allows you to use one Cisco ONS 15530 node in the network to monitor all the other Cisco ONS 15530 nodes in the network. The OSC is a point-to-point signal so any IP configuration valid for point-to-point interfaces is usable.

IP addressing on the OSC can be configured two ways:

- An IP address for each OSC wave interface with each address on a separate subnet.
- An unnumbered address for the OSC wave interfaces that reference another numbered interface.

The IP address of the reference interface is used as the IP packet source address. Use a loopback interface as the reference interface because it is always up. Configure IP address for each node in a separate subnet.



Note You can alternatively use the IP address of the NME (network management Ethernet) interface (fastethernet 0) for the reference address instead of the loopback interface.

To configure IP on an OSC wave interface, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface loopback 1 Switch(config-if)#	Selects the loopback interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# ip address <i>ip-address</i> <i>subnet-mask</i>	Configures IP address and subnet for the interface.
Step 3	Switch(config-if)# exit Switch(config)#	Exits interface configuration mode and returns to global configuration mode.
Step 4	Switch(config)# interface fastethernet 0 Switch(config-if)#	Selects the NME interface to configuration and enters interface configuration mode.
Step 5	Switch(config-if)# ip address <i>ip-address</i> <i>subnet-mask</i>	Configures IP address and subnet for the interface.
Step 6	Switch(config-if)# exit Switch(config)#	Exits interface configuration mode and returns to global configuration mode.
Step 7	Switch(config)# interface wave slot/0 Switch(config-if)#	Selects the wave interface in subcard 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 slot/1 Switch(config-if)#	Selects the wave interface in subcard 1.
Step 11	Switch(config-if)# ip unnumbered loopback 1	Configures an unnumbered interface referencing the loopback interface.

	Command	Purpose
Step 12	Switch(config-if)# exit Switch(config)#	Exits interface configuration mode and returns to global configuration mode.
Step 13	Switch(config)# ip route <i>prefix prefix-mask interface</i> or Switch(config)# router ospf <i>process-id</i> Switch(config-router)# network <i>network-address wildcard-mask area area-id</i> or Switch(config)# router eigrp <i>as-number</i> Switch(config-router)# network <i>network-number [network-mask]</i> or Switch(config)# router bgp <i>as-number</i> Switch(config-router)# network <i>network-number [mask network-mask]</i> Switch(config-router)# neighbor { <i>ip-address peer-group-name</i> } remote-as <i>number</i>	Configures IP static routes for some or all destinations. or Configures OSPF as the routing protocol. or Configures EIGRP as the routing protocol. or Configures BGP as the routing protocol.

**Note**

For detailed information about configuring routing protocols, refer to the [Cisco IOS IP and IP Routing Configuration Guide](#).

Example

The following example shows how to configure IP on the OSC on a three-node system. Node 1 connects to the NMS (network management system).

```

Node1# configure terminal
Node1(config)# interface loopback 1
Node1(config-if)# ip address 10.1.1.1 255.255.255.0
Node1(config-if)# exit
Node1(config)# interface fastethernet 0
Node1(config-if)# ip address 20.1.1.1 255.255.255.0
Node1(config-if)# exit
Node1(config)# interface wave 4/0
Node1(config-if)# ip unnumbered loopback 1
Node1(config-if)# exit
Node1(config)# interface wave 4/1
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 3/0
Node2(config-if)# ip unnumbered loopback 1
Node2(config-if)# exit
Node2(config)# interface wave 3/1
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 2/0
Node3(config-if)# ip unnumbered loopback 1
Node3(config-if)# exit
Node3(config)# interface wave 2/1
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

```

Displaying the OSC Configuration

To display the OSC configuration, use the following EXEC command:

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

Example

The following example shows the OSC configuration:

```

Switch# show interfaces wave 2/0
Wave2/0 is up, line protocol is up
  Channel: 0      Frequency: 191.9 Thz      Wavelength: 1562.23 nm
  Laser safety control: Off
  Osc physical port: Yes
  Wavelength used for inband management: No
  Configured threshold Group: None
  Last clearing of "show interface" counters never
  Hardware is OSC_phy_port
  Internet address is 1.0.0.3/16
  MTU 1492 bytes, BW 10000000 Kbit, DLY 0 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation SNAP, loopback not set
  Last input 00:00:01, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    13929 packets output, 919730 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out

```

Verifying Connectivity on the OSC

To verify connectivity over the OSC, use the following EXEC command:

Command	Purpose
<code>telnet ip-address</code>	Connects to another node using the reference IP address for the other node.

Example

The following example shows how to use Telnet to connect from node 1 to node 2 in the ring to another node through the OSC:

```
Node1# telnet 10.1.2.2
Trying 10.1.2.2 ... Open
Node2> enable
Node2#
```

Configuring IP on Ethernetdcc Interfaces for the In-Band Message Channel

Configuring IP on the in-band message channel allows you to use one Cisco ONS 15530 node in the network to monitor all the other Cisco ONS 15530 nodes in the network. The 2.5-Gbps ITU trunk cards, 10-Gbps ITU trunk cards, and the 10-Gbps uplink cards support the in-band message channel.

IP addressing for the in-band message channel can be configured in two ways:

- An IP address for each ethernetdcc interface with each address on a separate subnet.
- An unnumbered address for the Ethernet interfaces that reference another numbered interface.

The IP address of the reference interface is used as the IP packet source address. Use a loopback interface as the reference interface because it is always up. Configure IP address for each node in a separate subnet. Refer also to [“Interface Naming Conventions” section on page 2-4](#) for naming conventions.



Note You can alternatively use the IP address of the NME (network management Ethernet) interface (fastethernet 0) for the reference address instead of the loopback interface.

To configure IP on an ethernetdcc interface, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface loopback 1 Switch(config-if)#	Selects the loopback interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# ip address 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.

	Command	Purpose
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 ethernetccc slot/0/0 Switch(config-if)#	Selects the ethernetccc interface.
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)# ip route prefix prefix-mask interface or Switch(config)# router ospf process-id Switch(config-router)# network network-address wildcard-mask area area-id or Switch(config)# router eigrp as-number Switch(config-router)# network network-number [network-mask] or Switch(config)# router bgp as-number Switch(config-router)# network network-number [mask network-mask] Switch(config-router)# neighbor {ip-address peer-group-name} remote-as number	Configures IP static routes for some or all destinations. or Configures OSPF as the routing protocol. or Configures EIGRP as the routing protocol. or Configures BGP as the routing protocol.

**Note**

For detailed information about configuring routing protocols, refer to the [Cisco IOS IP and IP Routing Configuration Guide](#).

Example

The following example shows how to configure IP on the OSC on a three node system. Node 1 connects to the NMS (network management system).

```
Node1# configure terminal
Node1(config)# interface loopback 1
Node1(config-if)# ip address 10.1.1.1 255.255.255.0
Node1(config-if)# exit
Node1(config)# interface fastethernet 0
Node1(config-if)# ip address 20.1.1.1 255.255.255.0
```

```

Node1(config-if)# exit
Node1(config)# interface ethernetdcc 4/0/0
Node1(config-if)# ip unnumbered loopback 1
Node1(config-if)# exit

```

Displaying the Ethernetdcc Interface Configuration

To display the ethernetdcc interface configuration, use the following EXEC command:

Command	Purpose
<code>show interfaces ethernetdcc slot/subcard/port</code>	Displays the IP ethernetdcc interface configuration.

Example

The following example shows how to display the IP configuration:

```

Switch# show interfaces ethernetdcc 4/0/0
EthernetDcc10/0/0 is up, line protocol is up
  Hardware is cdl_enabled_port
  Interface is unnumbered. Using address of Loopback1 (10.1.1.1)
  MTU 1492 bytes, BW 500000 Kbit, DLY 0 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation SNAP, loopback not set
  Last input 00:00:02, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    26156 packets input, 1569630 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    22 packets output, 2436 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out

```

Verifying Connectivity over the In-Band Message Channel

To verify connectivity over the in-band message channel, use the following EXEC command:

Command	Purpose
<code>telnet ip-address</code>	Connects to another node using the reference IP address for the other node.

Example

The following example shows how to use Telnet to connect from node 1 to node 2 in the ring to another node through the in-band message channel:

```

Node1# telnet 10.1.2.2
Trying 10.1.2.2 ... Open
Node2> enable
Node2#

```


Configuring SNMP

SNMP is an application-layer protocol that allows an SNMP manager, such as 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 15530.

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 15530 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 CPU Switch Module Redundancy](#)” section on page 3-11.



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 15530 supports SMNP trap notifications through MIBs. This section describes the following MIBs:

- Alarm threshold MIB
- APS MIB
- CDL MIB
- Optical monitor MIB
- OSCP MIB
- Patch MIB
- Physical Topology MIB
- Redundancy facility MIB

You can find the complete list of MIBs supported on the Cisco ONS 15530 and the MIB definition files on the [Cisco MIB website](#) on Cisco.com. For more information on accessing the MIB definition files, refer to the [MIB Quick Reference for the Cisco ONS 15500 Series](#).

Alarm Threshold MIB

The interface alarm threshold MIB (CISCO-IF-THRESHOLD-MIB) assists SNMP monitoring of the interface alarm threshold activity. To enable the SNMP trap notifications for alarm threshold activity, use the following global configuration command:

Command	Purpose
<code>snmp-server enable traps threshold min-severity {degrade failure}</code>	Enables SNMP trap notifications for alarm threshold activity.

For information about other commands that enable SNMP trap notifications, refer to the [Cisco IOS Configuration Fundamentals Command Reference](#) publication.

Example

The following example shows how to enable SNMP trap notifications for alarm thresholds and set the minimum notification severity to signal degrade.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps threshold min-severity degrade
```

APS MIB

The APS MIB (CISCO-APS-MIB) assists SNMP monitoring of SONET APS activity. To enable the SNMP trap notifications for APS activity between associated interfaces, use the following global configuration command:

Command	Purpose
<code>snmp-server enable traps aps</code>	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
```

CDL MIB

The CDL MIB (CISCO-CDL-MIB) assists SNMP monitoring of the in-band message channel activity. To enable the SNMP trap notifications for the in-band channel, use the following global configuration command:

Command	Purpose
<code>snmp-server enable traps cdl {all terminating-interfaces} [soak-interval seconds]</code>	Enables SNMP trap notifications for the in-band message channel 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 all SNMP trap notifications for the in-band message channel activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps cdl all
```

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 <i>seconds</i>]	Enables SNMP trap notifications for network topology activity.

For information about other commands that enable SNMP trap notifications, refer to the [Cisco IOS Configuration Fundamentals Command Reference](#) publication.

Example

The following example shows how to enable SNMP trap notifications for network topology activity:

```
Switch# configure terminal
Switch(config)# snmp-server enable traps topology
```

Redundancy Facility MIB

The redundancy facility MIB (CISCO-RF-MIB) assists SNMP monitoring of processor redundancy activity. To enable the SNMP trap notifications for processor redundancy activity, use the following global configuration command:

Command	Purpose
snmp-server enable traps rf	Enables SNMP trap notifications for the redundancy facility activity.

For information about other commands that enable SNMP trap notifications, refer to the [Cisco IOS Configuration Fundamentals Command Reference](#) publication.

Example

The following example shows how to enable SNMP trap notifications for processor redundancy activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps rf
```

Monitoring Without the OSC or In-Band Message Channel

To take advantage of the OSC, the Cisco ONS 15530 system must be equipped with one OADM module with OSC (for unprotected configurations) or two OADM modules with OSC (for protected configurations). Likewise, to take advantage of the in-band message channel, the system must be equipped with a 2.5-Gbps ITU trunk card, 10-Gbps ITU trunk card, or a 10-Gbps uplink card. If your system is not equipped to support the OSC or in-band message channel, the following conditions apply:

- You cannot reach other nodes on the network using Telnet or SNMP. Separate connections to each system must exist on the network for management purposes.
- CDP does not function on the network. The physical topology must be configured manually for fault isolation and system management.
- Keepalive information is not available for other nodes on the network.

Setting up Connections to Individual Nodes

To access individual nodes in a Cisco ONS 15530 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.

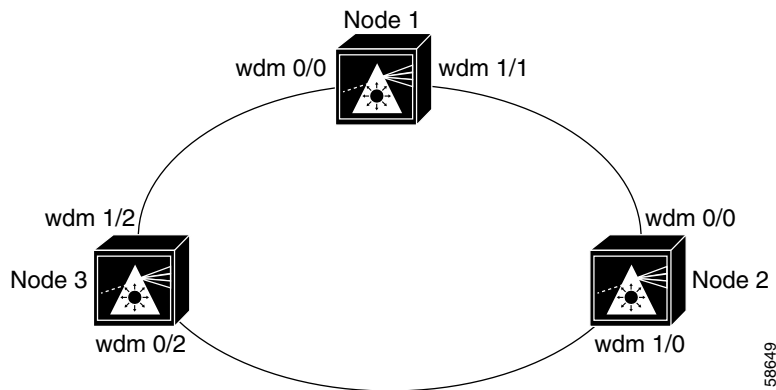
Manually Configuring the Network Topology

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}} [receive transmit]	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 12-2 shows an example ring topology with three shelves.

Figure 12-2 Ring Topology Example



The following example shows how to configure the network topology for node 1 in Figure 12-2:

```
Node1(config)# interface wdm 0/1
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 wdm0/1
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 12-2:

```
Node2(config)# interface wdm 0/0
Node2(config-if)# topology neighbor name Node1 port name wdm0/1
Node2(config-if)# topology neighbor agent ip-address 10.1.1.1
Node2(config)# exit
Node2(config)# interface wdm 0/1
Node2(config-if)# topology neighbor name Node3 port name wdm0/0
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 12-2:

```
Node3(config)# interface wdm 0/0
Node3(config-if)# topology neighbor name Node2 port name wdm0/1
Node3(config-if)# topology neighbor agent ip-address 10.2.2.2
Node3(config)# exit
Node3(config)# interface wdm 0/1
Node3(config-if)# topology neighbor name Node1 port name wdm0/0
Node3(config-if)# topology neighbor agent ip-address 10.1.1.1
```

Displaying the Network Topology

To display the network topology, use the following EXEC command:

Command	Purpose
<code>show topology neighbor</code>	Displays the network topology.

Example

The following example shows the network topology:

```
Switch# show topology neighbor
```

Physical Topology:

Local Port	Neighbor Node	Neighbor Port
Wd0/0	Node1	wdm0/0
Wd0/1	Node2	wdm0/1

Configuring Interfaces in the Network Topology

Not all interfaces on the Cisco ONS 15530 support CDP topology discovery, such as the transparent, esconphy, and wdmsplit interfaces. Also, not all equipment connected to a Cisco ONS 15530, such as EDFAs (erbium-doped fiber amplifiers) connected to wdm interfaces, support CDP. In these cases, you must explicitly add the interfaces to the network topology.

To add a interfaces to the network topology, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# interface { transparent <i>slot/subcard/0</i> wdm <i>slot/subcard</i> wdmsplit <i>slot/subcard</i> esconphy <i>slot/subcard/port</i> voain <i>slot/subcard/port</i> voaout <i>slot/subcard/port</i> voafilterin <i>slot/subcard/port</i> voafilterout <i>slot/subcard/port</i> } Switch(config-if)#	Selects the interface to configure and enters interface configuration mode.
Step 2	Switch(config-if)# topology neighbor { name <i>node-name</i> ip-address <i>node-ip-address</i> mac-address <i>node-mac-address</i> } { port { name <i>port-name</i> ip-address <i>port-ip-address</i> mac-address <i>port-mac-address</i> } } [receive transmit]	Configures the network topology information for a neighboring node.
Step 3	Switch(config-if)# topology neighbor agent ip-address <i>ip-address</i>	Specifies the address of the network topology agent on a neighboring node.

Example

The following example shows how to add a transparent interface to the network topology:

```
Switch(config)# interface transparent 8/0/0
Switch(config-if)# topology neighbor name router1 port name gigabitethernet1/1
Switch(config-if)# topology neighbor agent ip-address 10.1.1.1
```

Displaying Topology Information

To display the topology information, use the following EXEC command:

Command	Purpose
<code>show topology neighbor</code>	Displays network topology information.

Example

The following example shows how to display the client equipment topology:

```
Switch# show topology neighbor
```

```
Physical Topology:
```

```
Local Port      Neighbor Node      Neighbor Port
-----
Trans8/0/0     Router1            gigabitethernet1/1
```

About Embedded CiscoView

The Embedded CiscoView network management system provides a web-based interface for the Cisco ONS 15530. 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 15530 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 15530, perform the following steps:

	Command	Purpose
Step 1	Switch# <code>dir {bootflash: disk0:}</code>	Displays the contents of the specified Flash memory device, including the amount of free space that is available. If enough free space is available, skip to Step 4
Step 2	Switch# <code>delete {bootflash:filename diskn:filename}</code>	Deletes an old file to make room for the new file.
Step 3	Switch# <code>squeeze {bootflash:}</code>	Recovers the space on the Flash memory device.
Step 4	Switch# <code>copy tftp: {bootflash: disk0:}</code>	Copies the CiscoView tar file (ONS15530.tar) from the TFTP server. If you are installing Embedded CiscoView for the first time, skip to Step 6 .
Step 5	Switch# <code>delete {bootflash: disk0:}cv/*</code>	Removes existing files from the CiscoView directory.
Step 6	Switch# <code>archive tar /xtract disk0:ONS15530.tar {bootflash: disk0:}cv</code>	Extracts the CiscoView files from the tar file on the TFTP server to the CiscoView directory.

	Command	Purpose
Step 7	Switch# dir {bootflash: disk0:}	Displays the file in Flash memory. Repeat Step 4 and Step 7 for the file system on the standby processor (sby-bootflash: or sby-disk0:).
Step 8	Switch# configure terminal Switch(config)#	Enters global configuration mode.
Step 9	Switch(config)# ip http server	Enables the HTTP web server.
Step 10	Switch(config)# end Switch#	Returns to privileged EXEC mode.
Step 11	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 disk0:
Address or name of remote host []? 20.1.1.1
Source filename []? ONS15530.tar
Destination filename [ONS15530.tar]?
Accessing tftp://20.1.1.1/ONS15530.tar...
Loading ONS15530.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 disk0:ONS15530.tar disk0:/cv
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC

Switch# dir disk0:
Directory of disk0:/

   1  -rw-   2276396   Apr 30 2001 17:48:07  ONS15530-i-mz.121
   2  -rw-   1251840   May 23 2001 14:03:35  ONS15530.tar
   3  -rw-     8861   May 23 2001 14:26:05  cv/ONS15530-1.0.html
   4  -rw-  1183238   May 23 2001 14:26:06  cv/ONS15530-1.0.sgz
   5  -rw-     3704   May 23 2001 14:27:55  cv/ONS15530-1.0_ace.html
   6  -rw-     401   May 23 2001 14:27:55  cv/ONS15530-1.0_error.html
   7  -rw-    17003   May 23 2001 14:27:55  cv/ONS15530-1.0_jks.jar
   8  -rw-    17497   May 23 2001 14:27:57  cv/ONS15530-1.0_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-disk0:ONS15530.tar
Address or name of remote host []? 20.1.1.1
Source filename []? ONS15530.tar
Destination filename [ONS15530.tar]?
Accessing tftp://20.1.1.1/ONS15530.tar...
Loading ONS15530.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 disk0:ONS15530.tar sby-disk0:cv
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Switch# dir sby-disk0:
Directory of sby-disk0:/

   1  -rw-     2276396   May 20 2001 17:48:07  ONS15530-i-mz.121
   2  -rw-     1251840   May 23 2001 14:03:35  ONS15530.tar
   3  -rw-       8861   May 23 2001 14:26:05  cv/ONS15530-1.0.html
   4  -rw-     1183238   May 23 2001 14:26:06  cv/ONS15530-1.0.sgz
   5  -rw-       3704   May 23 2001 14:27:55  cv/ONS15530-1.0_ace.html
   6  -rw-        401   May 23 2001 14:27:55  cv/ONS15530-1.0_error.html
   7  -rw-     17003   May 23 2001 14:27:55  cv/ONS15530-1.0_jks.jar
   8  -rw-     17497   May 23 2001 14:27:57  cv/ONS15530-1.0_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 15530:

```
Switch# delete disk0:cv/*
Delete filename [cv/*]?
Delete disk0:cv/ONS15530-1.0.html? [confirm]
Delete disk0:cv/ONS15530-1.0.sgz? [confirm]
Delete disk0:cv/ONS15530-1.0_ace.html? [confirm]
Delete disk0:cv/ONS15530-1.0_error.html? [confirm]
Delete disk0:cv/ONS15530-1.0_jks.jar? [confirm]
Delete disk0:cv/ONS15530-1.0_nos.jar? [confirm]
Delete disk0:cv/applet.html? [confirm]
Delete disk0:cv/cisco.x509? [confirm]
Delete disk0:cv/identitydb.obj? [confirm]

Switch# copy tftp disk0:
Address or name of remote host []? 20.1.1.1
Source filename []? ONS15530.tar
Destination filename [ONS15530.tar]?
Accessing tftp://20.1.1.1/ONS15530.tar...
Loading ONS15530.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 disk0:ONS15530.tar disk0:cv
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC

Switch# delete sby-disk0:cv/*
Delete filename [cv/*]?
Delete disk0:cv/ONS15530-1.0.html? [confirm]
Delete disk0:cv/ONS15530-1.0.sgz? [confirm]
Delete disk0:cv/ONS15530-1.0_ace.html? [confirm]
Delete disk0:cv/ONS15530-1.0_error.html? [confirm]
Delete disk0:cv/ONS15530-1.0_jks.jar? [confirm]
Delete disk0:cv/ONS15530-1.0_nos.jar? [confirm]
Delete disk0:cv/applet.html? [confirm]
Delete disk0:cv/cisco.x509? [confirm]
Delete disk0:cv/identitydb.obj? [confirm]
Switch# copy tftp sby-disk0:
```

```

Address or name of remote host [20.1.1.1]?
Source filename [ONS15530.tar]?
Destination filename [ONS15530.tar]?
Accessing tftp://20.1.1.1/ONS15530.tar...
Loading ONS15530.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 disk0:ONS15530.tar disk0:cv
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Switch# archive tar /xtract tftp://10.1.1.1/ciscoview.tar sby-disk0:cv

```

Accessing Embedded CiscoView

Access Embedded CiscoView using the NME IP address as the URL for your Cisco ONS 15530 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:disk0:
CVFILE                               SIZE(in bytes)
-----
ONS15530-1.0.html                     8861
ONS15530-1.0.sgz                      1183238
ONS15530-1.0_ace.html                 3704
ONS15530-1.0_error.html               401
ONS15530-1.0_jks.jar                  17003
ONS15530-1.0_nos.jar                  17497
applet.html                           8861
cisco.x509                             529
identitydb.obj                        2523

Switch# show ciscoview version
Engine Version: 5.3 ADP Device: ONS15530 ADP Version: 1.0 ADK: 39

```




Numerics

10-Gbps ITU trunk cards

- configuring alarm thresholds [7-12 to 7-15](#)
- configuring interfaces [7-4](#)
- description [1-6](#)
- interfaces [2-6, 2-8](#)
- optical receive power thresholds [7-2, 7-5](#)
- splitter protection [10-3](#)

10-Gbps uplink cards

- configuring alarm thresholds [7-12 to 7-15](#)
- configuring interfaces [7-7](#)
- description [1-6](#)
- interfaces [2-10](#)

2.5-Gbps ITU trunk cards [1-5, 4-1](#)

- configuring alarm thresholds [4-9, 7-12 to 7-15](#)
- configuring cross connections [4-8, 5-10, 7-10](#)
- configuring interfaces [7-1](#)
- configuring patch connections [7-15](#)
- description [1-5](#)
- displaying interface configuration [7-3](#)
- interfaces [2-6](#)
- laser safety control [6-16](#)

8-port FC/GE aggregation cards

- description [1-4](#)
- forward laser control support [5-4](#)
- interfaces [2-5](#)

A

AAA

- configuring [3-9](#)

alarm thresholds

- configuring [4-9, 5-11, 6-11](#)
- description [4-9, 5-11, 6-10, 7-11](#)
- displaying configuration [6-13](#)
- MIBs [12-15](#)
- rates (table) [4-10, 5-12, 6-12, 7-12](#)

ALS

- laser safety control and [6-16](#)

amplifiers. See EDFAs

APS

- configuring line card protection [10-11 to 10-13](#)
- configuring multiple shelf nodes [11-3 to 11-5](#)
- configuring splitter protection [10-5 to 10-7](#)
- lockouts [10-29 to 10-32](#)
- MIBs [12-16](#)
- switchovers [10-29 to 10-32](#)

aps clear command [10-31](#)

aps direction command [10-23](#)

aps disable command [10-20, 10-23, 11-3](#)

aps enable command [9-2, 10-5, 10-11, 10-15, 10-17, 10-20, 10-23, 10-28, 11-3](#)

aps far-end command [11-3](#)

aps lockout command [10-30](#)

APS lockouts. See lockouts

aps message-channel command [9-2, 10-17](#)

aps protection command [9-2, 10-5, 10-11, 10-15, 10-17, 11-3](#)

aps revertive command [10-20](#)

aps switch command [10-30](#)

APS switchovers. See switchovers

aps timer message-channel command [10-23](#)

aps timer message max-interval command [10-23](#)

aps timer oscp holddown command [10-23](#)

aps timer search-for-up command [10-28](#)

aps timer wait-to-restore command [10-20](#)
 aps trigger command [6-11](#)
 aps working command [9-2, 10-5, 10-11, 10-15, 10-17, 11-3](#)
 aps y-cable command [10-11, 11-3](#)
 associate group command [9-2, 10-5, 10-11, 10-14, 10-17, 10-19, 10-23, 11-3](#)
 attenuation
 automatic [8-6](#)
 manual [8-6](#)
 Authentication, Authorization, and Accounting. See AAA
 autoboot
 configuring [3-17](#)
 displaying configuration [3-17](#)
 See also booting
 automatic laser shutdown. See ALS
 Automatic Protection Switching. See APS
 automatic synchronization
 causes (table) [3-19](#)
 configuring [3-18](#)
 auto-sync running-config command [3-19](#)
 auto-sync startup-config command [3-19](#)
 auxiliary ports
 interface naming convention [2-16](#)
 modem support [3-3](#)

B

bidirectional path switching
 configuring [10-23](#)
 description [10-22](#)
 displaying configuration [10-27](#)
 example (figure) [10-24, 10-25](#)
 figure [10-22](#)
 boot command [3-27](#)
 booting
 default behavior [3-27](#)
 bootstrap failure
 system response [3-26](#)
 boot system command [3-17](#)

Break key
 controlling [3-25](#)

C

carrier motherboard
 description [1-8](#)
 carrier motherboards
 description [1-7](#)
 cdl defect-indication force hop-endpoint command [7-2, 7-4, 7-7](#)
 cdl flow-identifier command [4-3](#)
 cdl flow-identifier reserved command [4-3](#)
 CDP
 clearing information [12-5](#)
 configuring [12-3 to 12-6](#)
 description [12-3](#)
 displaying configuration [12-3](#)
 displaying information [12-4](#)
 cdp advertise-v2 command [12-3](#)
 cdp holdtime command [12-3](#)
 cdp run command [12-3](#)
 cdp timer command [12-3](#)
 channels
 description [1-6](#)
 OSC [1-10](#)
 See also data channels
 Cisco Discovery Protocol. See CDP
 Cisco ONS 15216 OADMs
 APS switching [10-23](#)
 path switching example (figure) [10-25](#)
 Cisco ONS 15530
 configuration overview [2-20](#)
 starting up [3-2](#)
 See also hardware; shelf; software
 Cisco Transport Manager. See CTM
 CiscoView. See Embedded CiscoView
 clear cdp counters command [12-5](#)
 clear cdp table command [12-5](#)

CLI

- description [2-1](#)

- help [2-3](#)

client equipment

- monitoring [12-21](#)

client protection

- configuring [10-7](#)

- description [10-7](#)

- See also line card protection; y-cable protection

client signals

- esconphy interfaces and [2-5](#)

- gigabitphy interfaces [2-6](#)

- transparent interfaces and [2-12](#)

clock rate command [6-3](#)

command-line interface. See CLI

command modes

- description [2-1](#)

- table [2-2](#)

commands

- abbreviating [2-3](#)

- listing [2-3](#)

- syntax in documentation [xiv](#)

compliance

- support [1-11](#)

components

- description [1-3 to 1-9](#)

config-register command [3-17, 3-28](#)

configuration register

- changing value [3-17](#)

- See software configuration register

configurations

- displaying [3-6](#)

- overview of tasks [2-20](#)

- synchronizing [3-18 to 3-19](#)

connect command [4-8, 5-10, 7-10](#)

console ports

- configuring modem support [3-2](#)

- using [3-2](#)

- See also NME

conventions

- document [xv](#)

- naming interfaces [2-4 to 2-20](#)

CPUs. See CPU switch modules

CPU switch module redundancy. See redundancy

CPU switch modules

- autoboot [3-17](#)

- configuring [3-15 to 3-23](#)

- description [1-8, 3-1](#)

- hardware state transitions [3-12](#)

- interfaces [2-16](#)

- redundant [3-15](#)

- reloading [3-23](#)

- slot assignments [1-3](#)

- software state transitions [3-13](#)

- starting up [3-2](#)

CPU switch module switchovers

- forcing [3-15 to 3-16](#)

cross connections

- configuring across switch fabric [4-8, 5-10, 7-10](#)

- description [4-7, 5-9, 7-9](#)

- display configuration [4-9, 5-10, 7-11](#)

- displaying [6-23](#)

- transponder line cards [6-23](#)

CTM

- support [1-10](#)

D

data channels

- OSC and [1-10, 12-1](#)

- See also channels

description command [4-10, 5-11, 6-11, 7-12](#)

diagnostic tests. See online diagnostics

digital video. See DV

documentation

- conventions [xv](#)

- related [xiv](#)

duplex command [3-5](#)

DV

support on transponder line cards [6-4](#)

E

EDFAs

monitoring [12-21](#)

Embedded CiscoView

accessing [12-25](#)

description [12-22](#)

download URL [12-22](#)

installing [12-22 to 12-25](#)

support [1-10](#)

enable password command [3-4](#)

enable passwords

description [3-3](#)

enable secret command [3-4](#)

enable secret passwords

description [3-3](#)

encapsulation command [6-3](#)

environment-monitor shutdown fan command [3-29](#)

erbium-doped fiber amplifiers. See EDFAs

ESCON

configuring protocol encapsulation (table) [6-3](#)

ESCON aggregated signals

configuring [4-2, 5-1](#)

ESCON aggregation card

forward laser control support [4-4](#)

ESCON aggregation cards

description [1-4](#)

interfaces [2-4](#)

signal aggregation support [4-1](#)

esconphy interfaces

configuring [4-3](#)

configuring alarm thresholds [4-9 to 4-11, 5-11 to 5-13](#)

configuring cross connection [4-8, 5-10, 7-10](#)

description [2-5](#)

displaying configuration [4-4](#)

ethernetdcc interfaces

configuring IP [12-12 to 12-14](#)

description [2-7, 2-9, 2-11](#)

Ethernet management ports. See NME

F

fan failure shutdown

configuring [3-29](#)

description [3-29](#)

displaying configuration [3-30](#)

Fast Ethernet

configuring protocol encapsulation (table) [6-3](#)

fastethernet 0 interfaces

configuring [3-4 to 3-6](#)

configuring IP addresses [3-4](#)

description [2-16](#)

IP on in-band message channel [12-12](#)

IP on OSC [12-9](#)

See also NME

fastethernet-sby 0 interfaces

description [2-16](#)

See also NME

FDDI

configuring protocol encapsulation (table) [6-3](#)

Fibre Channel

configuring protocol encapsulation (table) [6-3](#)

FICON

configuring protocol encapsulation (table) [6-3](#)

filter interfaces

description [2-14](#)

firewalls

configuring [3-11](#)

Flash PC Cards

displaying contents [12-22](#)

flow control command [5-4](#)

forward laser control

configuring on esconphy interfaces [4-3](#)

configuring on gigabitphy interfaces [5-4](#)

configuring on transparent and wave interfaces [6-17](#)
 description [6-14](#)
 displaying configuration [6-18](#)
 figure [6-14](#)
 OFC and (caution) [6-17](#)

G

Gigabit Ethernet
 configuring protocol encapsulation (table) [6-3](#)
 gigabitphy interfaces
 description [2-6](#)

H

hardware
 components [1-3 to 1-9](#)
 features [1-2 to 1-9](#)
 OSC guidelines [12-2](#)
 shelf overview [1-3](#)
 Hello hold-down timer
 configuring [12-7](#)
 Hello inactivity factor
 configuring [12-7](#)
 Hello interval timer
 configuring [12-6](#)
 help
 CLI [2-3](#)
 hostname command [3-6](#)
 host names
 configuring [3-6](#)

I

in-band message channel
 configuring IP [12-12 to 12-14](#)
 description [1-11](#)
 displaying configuration [12-14](#)

MIBs [12-16](#)
 verifying connectivity [12-14](#)
 interface ethernetdcc command [12-13](#)
 interface loopback command [12-9, 12-12](#)
 interfaces
 naming conventions [2-4 to 2-20](#)
 OSC modules [2-16](#)
 See also specific types of interfaces (for example, filter interfaces)
 interface transparent command [6-3](#)
 interface wave command [6-18, 6-20, 9-7, 9-8, 12-9](#)
 interface wdm command [12-19](#)
 IP
 configuring on OSC interfaces [12-8 to 12-12](#)
 configuring over in-band message channel [12-12 to 12-14](#)
 ip address command [3-4, 12-9, 12-12](#)
 IP addresses
 configuring on NME [3-4](#)
 ethernetdcc interfaces [12-12](#)
 OSC wave interfaces [12-8](#)
 ip route command [12-10, 12-13](#)
 ip unnumbered command [12-9, 12-13](#)

K

Kerberos
 configuring [3-9](#)

L

laser control. See forward laser control; laser safety control
 laser control forward enable command [6-17](#)
 laser control safety enable command [6-18, 7-2](#)
 laser frequency command [6-6, 7-1](#)
 laser safety control
 configuring [6-18](#)
 description [6-16](#)
 displaying configuration [6-19](#)

figure [6-16](#)
 line card protection and [6-18](#)
 OFC and (caution) [6-18](#)
 splitter protection and (caution) [6-16, 10-5](#)

laser shutdown

configuring [6-17 to 6-19](#)
 description [6-14 to 6-16](#)

laser shutdown command [7-2, 7-4, 7-7](#)

line card protection

configuring y-cable protection [10-11](#)
 considerations [10-10, 10-14](#)
 description [10-7](#)
 displaying cross connections (example) [6-23](#)
 example (figure) [10-8, 10-9](#)
 lockouts [10-29 to 10-32](#)
 switchovers [10-29 to 10-32](#)

See also y-cable protection

line card redundancy controllers. See LRCs

line vty command [3-5](#)

lockouts

clearing [10-31](#)
 description [10-29](#)
 displaying status [10-30, 10-31](#)
 requesting [10-30](#)

loopback command [7-1, 7-4, 7-7](#)

LRCs

description [1-8](#)

M

maintenance-mode command [3-20](#)

management ports. See NME

management systems. See network management systems

meshed ring topologies. See network topologies

MIBs

enabling SNMP notifications [12-15 to 12-18](#)
 support [3-1](#)
 supported [12-15](#)

modem

support [3-3](#)

monitor enable command [6-9](#)

monitoring. See network monitoring; protocol monitoring

multiple shelf nodes

configuring [11-1 to 11-5](#)
 description [11-1](#)

mux/demux modules. See OADM modules

N

negotiation auto command [5-4](#)

network management Ethernet. See NME

network management systems

supported [1-10](#)
 See also Embedded CiscoView

network monitoring

CDP [12-3 to 12-5](#)
 Embedded CiscoView [12-22 to 12-25](#)
 OSCP [12-6 to 12-8](#)
 transparent interfaces [12-21](#)
 wdm interfaces [12-21](#)
 without OSC or in-band message channel [12-19 to 12-21](#)

Network Time Protocol. See NTP

network topologies

adding interfaces [12-21](#)
 adding wdm interfaces [12-5](#)
 MIBs [12-17, 12-18](#)
 types [1-11](#)

NME

configuring interfaces [3-4](#)
 description [2-16](#)
 displaying configuration [3-5](#)
 using [3-2](#)

See also fastethernet 0 interfaces

notification-throttle timer command [4-9, 5-11, 6-11, 7-12](#)

NTP

configuring [3-7](#)

- description [3-7](#)
- displaying configuration [3-8](#)
- ntp server command [3-8](#)
- ntp update-calendar command [3-8](#)

O

OADM modules

- configuring for line card protection [10-11](#)
- description [1-7](#)
- interfaces [2-13](#)

OFC

- configuring with encapsulation command [6-3](#)
- description [6-15](#)
- figure [6-15](#)
- forward laser control and (caution) [6-17](#)
- laser safety control and (caution) [6-18](#)

online diagnostics

- description [1-11](#)

open fiber control. See OFC

optical attenuation automatic desired-value command [8-6](#)

optical attenuation manual command [8-7](#)

optical connections. See cross connections

optical monitor

- MIBs [12-17](#)

optical power thresholds

- configuring [6-19, 7-2, 7-5, 8-8, 9-7](#)
- displaying configuration [6-20, 9-8](#)
- trunk fiber based protection switchovers [9-3 to 9-7](#)

optical supervisory channel. See OSC

Optical Supervisory Channel Protocol. See OSCP

optical threshold power receive command [6-20, 7-2, 7-5, 8-9, 9-7, 9-8](#)

optical thresholds

- description [8-8](#)

OSC

- description [1-10, 12-1 to 12-2](#)
- hardware guidelines [12-2](#)
- OSCP [12-6 to 12-8](#)

- signal path (figure) [12-2](#)
- types of information [1-10](#)
- verifying configuration [12-11](#)
- verifying connectivity [12-12](#)

oscfiler interfaces

- configuring patch connections [6-21](#)
- description [2-14](#)

OSC interfaces

- configuring CDP [12-3 to 12-5](#)
- configuring IP [12-8 to 12-12](#)
- patch connections [6-21](#)

OSC modules

- description [1-8](#)
- interfaces [2-16](#)

OSCP

- configuring [12-6 to 12-7](#)
- description [12-2](#)
- displaying configuration [12-8](#)
- displaying neighbors [12-8](#)
- MIBs [12-17](#)

OSC Protocol. See OSCP

oscp timer hello holddown command [12-7](#)

oscp timer hello interval command [12-7](#)

oscp timer inactivity-factor command [12-7](#)

P

passwords

- description [3-3](#)

patch connections

- configuring for PSMs [9-9 to 9-10](#)
- configuring for transponder line cards [6-2, 6-21 to 6-22](#)
- configuring for trunk cards [7-15](#)
- description [6-21](#)
- displaying configuration [6-22, 9-9](#)
- types (table) [6-21](#)

path lockouts. See lockouts

path switching

- configuring [10-23 to 10-27](#)
- description [10-21 to 10-23](#)

See also bidirectional path switching; unidirectional path switching

path switchovers. See switchovers

PB-OE modules

- automatic attenuation [8-6](#)
- configuring [8-5](#)
- description [1-8, 8-3](#)
- dual band [8-4](#)
- manual attenuation [8-6](#)
- single band [8-3](#)

per-band optical equalizer modules. See PB-OE modules

point-to-point topologies. See network topologies

portgroup interfaces

- description [2-5, 2-6](#)

power equalization

- figure [8-2](#)

processors. See CPU switch modules

protection

- types [10-2 to 10-13](#)

protection switching. See path switching

protocol encapsulation

- configuring [6-2 to 6-5](#)
- types supported [1-6](#)

protocol monitoring

- configuring [6-9](#)
- description [6-7](#)
- displaying configuration [6-9](#)

Q

quick laser shutdown. See forward laser control; laser safety control

R

RADIUS

- configuring [3-10](#)

redundancy

- configuring [3-15 to 3-23](#)
- description [3-11 to 3-14](#)
- displaying alarm status (note) [3-12](#)
- displaying configuration [3-20](#)
- forcing switchovers [3-15 to 3-16](#)
- hardware state transitions [3-12](#)
- MIBs [12-18](#)
- software state transitions [3-13](#)
- synchronizing configurations [3-18](#)

redundancy command [3-19, 10-5](#)

redundancy manual-sync command [3-18](#)

redundancy reload peer command [3-23](#)

redundancy reload shelf command [3-23](#)

redundancy switch-activity command [3-15](#)

reset command [3-16](#)

reshape, retime, retransmit functions. See 3R functions

revertive switching

- configuring [10-19](#)
- description [10-19](#)
- displaying configuration [10-20](#)

router bgp command [12-10, 12-13](#)

router eigrp command [12-10, 12-13](#)

router ospf command [12-10, 12-13](#)

S

SDH

- configuring protocol encapsulation (table) [6-3](#)

security features

- AAA [3-9](#)
- firewalls [3-11](#)
- Kerberos [3-9](#)
- overview [3-8](#)
- passwords and privileges [3-11](#)

- RADIUS [3-10](#)
- TACACS+ [3-10](#)
- traffic filters [3-11](#)
- shelf
 - configuration overview [2-20](#)
 - description [1-3](#)
 - layout (figure) [1-3](#)
 - starting up [3-2](#)
- show aps command [9-3, 10-6, 10-12, 10-15](#)
- show bootvar command [3-17](#)
- show cdp command [12-3](#)
- show cdp entry command [12-4](#)
- show cdp interface command [12-4](#)
- show cdp neighbor command [12-4](#)
- show cdp traffic command [12-4](#)
- show ciscoview package command [12-25](#)
- show ciscoview version command [12-25](#)
- show connect command [4-9, 5-10, 6-23, 7-11](#)
- show environment command [3-30](#)
- show flash command [12-22](#)
- show hardware command [3-4](#)
- show ntp status command [3-8](#)
- show oscp info command [12-8](#)
- show oscp neighbor command [12-8](#)
- show patch command [6-22, 9-9](#)
- show redundancy capability command [3-20](#)
- show redundancy running-config-file command [3-20](#)
- show redundancy summary command [3-20, 3-23](#)
- show threshold-list command [4-11, 5-12, 6-13, 7-13](#)
- show topology command [9-11, 12-6, 12-22](#)
- show topology neighbor command [12-20](#)
- show version command [3-17](#)
- Simple Network Management Protocol. See SNMP
- SNMP
 - configuring [12-15](#)
 - configuring alarm thresholds (table) [4-9, 5-11, 7-12](#)
 - support [3-1](#)
- snmp-server enable traps aps command [12-16](#)
- snmp-server enable traps cdl command [12-16](#)
- snmp-server enable traps optical monitor command [12-17](#)
- snmp-server enable traps oscp command [12-17](#)
- snmp-server enable traps patch command [12-17](#)
- snmp-server enable traps rf command [12-18](#)
- snmp-server enable traps threshold min-severity command [12-15](#)
- snmp-server enable traps topology command [12-18](#)
- software
 - features [1-9 to 1-11](#)
- software configuration register
 - boot field values [3-26](#)
 - Break key, controlling [3-25](#)
 - changing [3-28](#)
 - description [3-24](#)
 - IP broadcast address [3-25](#)
 - response to bootload failure [3-26](#)
 - settings [3-25](#)
 - verifying value [3-28](#)
- SONET
 - configuring protocol encapsulation (table) [6-3](#)
- SONET APS. See APS
- speed command [3-4](#)
- splitter protection
 - configuring [10-5](#)
 - considerations [10-4](#)
 - description [10-2, 10-5](#)
 - displaying configuration [10-6](#)
 - displaying cross connections (example) [6-23](#)
 - example (figure) [10-3](#)
 - lockouts [10-29 to 10-32](#)
 - switchovers [10-29 to 10-32](#)
- SRCs
 - description [1-8](#)
- standards compliance. See compliance
- standby CPU switch modules
 - enabling privileged EXEC mode access [3-23](#)
- standby privilege-mode enable command [3-23](#)
- switchcard redundancy controllers. See SRCs

- switch fabric based protection
 - configuring [10-14](#)
 - description [10-13](#)
 - displaying configuration [10-15](#)
 - example (figure) [10-13](#)
 - switch fabrics
 - description [1-9](#)
 - redundant [10-18](#)
 - redundant (figure) [10-19](#)
 - switchover command [3-15](#)
 - switchover-enable timer
 - configuring [10-27](#)
 - displaying configuration [10-28](#)
 - switchovers
 - clearing [10-31](#)
 - description [10-29](#)
 - displaying status [10-30, 10-31](#)
 - requesting [10-30](#)
 - types [10-29](#)
 - synchronizing
 - configurations [3-18 to 3-19](#)
 - Synchronous Digital Hierarchy. See SDH
 - system management
 - TACACS [3-10](#)
-
- T**
- TACACS [3-10](#)
 - TACACS+
 - configuring [3-10](#)
 - telnet command [12-12, 12-14](#)
 - tengigethernetphy interfaces
 - configuring [7-7](#)
 - description [2-11](#)
 - displaying configuration [7-8](#)
 - tengigethernetphy subinterfaces
 - configuring cross connections [4-8, 5-10, 7-10](#)
 - description [2-11](#)
 - displaying configuration [7-8](#)
 - threshold command [4-10, 5-11, 6-11, 7-12](#)
 - threshold-group command [4-10, 5-11, 6-11, 7-12](#)
 - threshold-list command [4-9, 5-11, 6-11, 7-12](#)
 - thresholds. See alarm thresholds
 - thresholds. See optical power thresholds
 - thru interfaces
 - configuring patch connections [6-21](#)
 - description [2-15](#)
 - topologies. See network topologies. hubbed ring topologies. See network topologies
 - topology hold-time command [12-5](#)
 - topology neighbor agent ip-address command [9-10, 9-11, 11-2, 12-19, 12-21](#)
 - topology neighbor cdp command [12-5](#)
 - topology neighbor command [9-10, 9-11, 11-2, 12-19, 12-21](#)
 - topology neighbor disable command [12-5](#)
 - traffic filters
 - configuring [3-11](#)
 - transparent interfaces
 - adding to network topology [12-21](#)
 - configuration overview [6-1](#)
 - configuring alarm thresholds [6-10 to 6-13](#)
 - configuring protocol encapsulation [6-2 to 6-5](#)
 - description [2-12](#)
 - displaying network topology information [9-11, 12-22](#)
 - transponder line cards
 - configuring laser frequency [6-6](#)
 - configuring protocol monitoring [6-9](#)
 - configuring y-cable protection [10-11](#)
 - description [1-6](#)
 - interfaces [2-12](#)
 - line card protection example (figure) [10-8](#)
 - optical link loss (table) [4-5, 4-6, 5-6, 5-8](#)
 - protocol encapsulation support [1-6](#)
 - protocol monitoring support [6-7](#)
 - shutting down lasers [6-14 to 6-19](#)
 - splitter protection and [10-4](#)
 - splitter protections (figure) [10-2](#)
 - types [1-6](#)

troubleshooting

- cross connections [6-23](#)
- online diagnostics [1-11](#)
- shelf misconfigurations [6-22](#)

trunk fiber based protection

- configuring wdm split interfaces [9-2](#)
- switchovers and optical power thresholds [9-3 to 9-7](#)

trunk fiber protection

- considerations [10-17](#)
- description [10-16](#)

tx-buffer size command [4-6, 5-7](#)

U

unidirectional path switching

- configuring [10-23](#)
- description [10-22](#)
- displaying configuration [10-27](#)
- example (figure) [10-22](#)

V

value command [4-10, 5-11, 6-11, 7-12](#)

variable optical attenuation

- description [8-1](#)

variable optical attenuations

- example (figure) [8-2](#)

variable optical attenuator modules. See VOA modules

voafilterin interfaces

- configuring automatic attenuation [8-6](#)
- configuring manual attenuation [8-6](#)
- configuring optical thresholds [8-8](#)
- displaying configuration [8-7](#)

voain interfaces

- configuring automatic attenuation [8-6](#)
- configuring manual attenuation [8-6](#)
- configuring optical thresholds [8-8](#)
- displaying configuration [8-7](#)

VOA modules

- configuring [8-5](#)
- description [1-8, 8-2](#)
- types [1-8, 8-2](#)

See also PB-OE modules; WB-VOA modules

W

waveethernetphy interfaces

- configuring [7-1, 7-4](#)
- description [2-7, 2-9](#)
- displaying configuration [7-3, 7-5](#)

waveethernetphy subinterfaces [2-10](#)

- configuring [7-4](#)
- configuring cross connections [4-8, 5-10, 7-10](#)
- displaying configuration [7-5](#)

wave interface

- description [2-16](#)

wave interfaces

- configuration overview [6-2](#)
- configuring alarm thresholds [6-10 to 6-13](#)
- configuring forward laser control [6-17](#)
- configuring laser safety control [6-18](#)
- configuring patch connections [6-21](#)
- description [2-13](#)

wavepatch interfaces

- description [2-7, 2-10, 2-13](#)

WB-VOA modules

- automatic attenuation [8-6](#)
- configuring [8-5](#)
- description [1-8, 8-2](#)
- dual [8-3](#)
- manual attenuation [8-6](#)
- single [8-2](#)

wdm interfaces

- adding manually to network topologies, example [12-19 to 12-21](#)
- adding to network topology [12-21](#)
- configuring CDP [12-5](#)

- configuring patch connections [6-21](#)
- description [2-14](#)
- displaying CDP information [12-6](#)
- displaying network topology information [12-22](#)
- wdmrelay interfaces
 - configuring patch connections [9-9](#)
- wdmsplit interface
 - enabling [9-1](#)
- wdmsplit interfaces
 - displaying information [9-2](#)
- wide-band variable optical attenuator modules. See
WB-VOA modules

Y

- y-cable protection
 - configuring [10-11](#)
 - considerations [10-10](#)
 - description [10-9](#)
 - displaying configuration [10-12](#)