CISCO SYSTEMS

Cisco ONS 15540 ESPx Command Reference Guide

Cisco IOS Release 12.2SV
February 2006

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

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

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

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

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

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

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

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

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

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

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

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

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

Cisco ONS 15540 ESPx Command Reference Guide
© 2006 Cisco Systems, Inc. All rights reserved.

C O N T E N T S

CHAPTER 2   **Debug Commands**   **2-1**

CHAPTER 3   **Interface Configuration Commands**   **3-1**

T A B L E S

Preface

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

This section provides the following information:

- Document Objectives
- Audience
- Document Organization
- Related Documentation
- About the CLI
- About Cisco IOS Command Modes
- Document Conventions
- Where to Find Safety and Warning Information
- Obtaining Documentation
- Documentation Feedback
- Cisco Product Security Overview
- Obtaining Technical Assistance
- Obtaining Additional Publications and Information

Document Objectives

This guide explains the commands to configure and manage the Cisco ONS 15540 ESPx system. Use this guide in conjunction with the appropriate publications listed in the Related Documentation section.

Audience

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

Document Organization

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

- Chapter 1, "APS Commands," lists the commands to configure and monitor APS operations.
- Chapter 2, "Debug Commands," lists the commands to debug the Cisco ONS 15540 ESPx.
- Chapter 3, "Interface Configuration Commands," lists the commands to configure and monitor the interfaces on the Cisco ONS 15540 ESPx.
- Chapter 4, "Online Diagnostics Commands," lists the commands to configure and monitor online diagnostic operations.
- Chapter 5, "OSCP Commands," lists the commands to configure and monitor OSCP operations.
- Chapter 6, "Processor Card Redundancy Commands," lists the commands to configure and monitor processor card redundancy operations.
- Chapter 7, "SNMP Commands," lists the Cisco ONS 15540 ESPx-specific SNMP commands.
- Chapter 8, "System Management Commands," lists the commands to manage your Cisco ONS 15540 ESPx.
- Chapter 9, "Threshold Commands," lists the commands to configure and monitor interface alarm threshold operations.
- Chapter 10, "Topology Neighbor Commands," lists the commands to configure and monitor network topology neighbors.

Related Documentation

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

- *Regulatory Compliance and Safety Information for the Cisco ONS 15500 Series*

  Provides the regulatory compliance and safety information for the Cisco ONS 15500 Series.

- *Cisco ONS 15540 ESPx Planning Guide*

  Provides detailed information on the Cisco ONS 15540 ESPx architecture and functionality.

- *Cisco ONS 15540 ESPx Hardware Installation Guide*

  Provides detailed information about installing the Cisco ONS 15540 ESPx.

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

  Provides acceptance testing procedures for Cisco ONS 15540 ESPx nodes and networks.

- *Cisco ONS 15540 ESPx Cleaning Procedures for Fiber Optic Connections*

  Provides processes and procedures for cleaning the fiber optic connectors and component interfaces of the Cisco ONS 15540 ESPx.

- *Cisco ONS 15540 ESPx Configuration Guide*

  Describes how to configure the Cisco ONS 15540 ESPx.

- *Cisco ONS 15540 ESPx System Alarms and Error Messages*

  Describes the system alarms and error messages for the Cisco ONS 15540 ESPx.

- *Cisco ONS 15540 ESPx Troubleshooting Guide*

Describes how to identify and resolve problems with the Cisco ONS 15540 ESPx.

- *Network Management for the Cisco ONS 15540 ESPx*

  Provides information on the network management systems that support the Cisco ONS 15540 ESPx.

- *Cisco ONS 15540 ESPx TL1 Commands*

  Provides a full TL1 command and autonomous message set including parameters, AIDs, conditions and modifiers for the Cisco ONS 15540 ESPx.

- *MIB Quick Reference for the Cisco ONS 15500 Series*

  Describes the Management Information Base (MIB) objects and explains how to access Cisco public MIBs for the Cisco ONS 15500 Series.

- *Cisco ONS 15540 ESPx Software Upgrade Guide*

  Describes how to upgrade system images and functional images on the Cisco ONS 15540 ESPx.

- *Introduction to DWDM Technology*

  Provides background information on the dense wavelength division multiplexing (DWDM) technology.

- *Cisco IOS Configuration Fundamentals Configuration Guide*

  Provides useful information on the CLI (command-line interface) and basic shelf management.

About the CLI

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

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

About Cisco IOS Command Modes

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

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

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

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

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

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

Table 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 1   *Frequently Used IOS Command Modes*

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

Table 1   Frequently Used IOS Command Modes (continued)

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

1. Automatic Protection Switching

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

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

Listing Cisco IOS Commands and Syntax

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

```
Switch> ?
```

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

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

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

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

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

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

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

Document Conventions

This publication uses the following conventions:

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

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

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

Warning **IMPORTANT SAFETY INSTRUCTIONS**

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

SAVE THESE INSTRUCTIONS

Where to Find Safety and Warning Information

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

Obtaining Documentation

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

Cisco.com

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

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

Cisco Optical Networking Product Documentation CD-ROM

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

Ordering Documentation

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

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

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

Documentation Feedback

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

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

- Report security vulnerabilities in Cisco products.

- Obtain assistance with security incidents that involve Cisco products.

- Register to receive security information from Cisco.

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

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

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

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

Reporting Security Problems in Cisco Products

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

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

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

- For Nonemergencies — psirt@cisco.com

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

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

$\mathcal{Q}$

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

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

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

http://www.cisco.com/techsupport

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

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

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

Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

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

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

  http://www.ciscopress.com

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

  http://www.cisco.com/packet

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

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

  or view the digital edition at this URL:

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

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

  http://www.cisco.com/ipj

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

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

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

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

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

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

APS Commands

APS (Automatic Protection Switching) provides protection against signal failure. Use the following commands to configure and monitor APS operations.

aps clear

To clear an APS switchover request or an APS lockout request, use the **aps clear** command.

aps clear *group-name*

Syntax Description

group-name	Specifies the name of the associated pair of interfaces.

Defaults None

Command Modes Privileged EXEC

Command History This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines The Cisco ONS 15540 ESPx supports APS signal switchover requests from the CLI (command-line interface). These requests have priorities depending on the condition of the protection signal and whether another switchover or lockout request is in effect. There are three types of requests:

- Lockout requests—Have the highest priority and take effect regardless of the condition of the protection signal. A lockout prevents the signal from switching over from the working interface to the protection interface.
- Forced switchover requests—Have the next highest priority and are only prevented if there is an existing lockout on the protection interface, or the protection signal has failed.
- Manual switchover requests—Have the lowest priority and only occur if there is no protection path lockout, a forced switchover, or the signal has failed or degraded.

Examples The following example shows how to clear an APS request on an associated interface pair named blue.

```
Switch# aps clear blue
```

The following example shows how to clear an APS request for an associated interface pair with the default group name.

```
Switch# aps clear Wavepatch2/0/0
```

Related Commands	Command	Description
	aps lockout	Prevents switchovers to the protection path.
	aps switch	Requests an APS switchover.
	show aps	Displays APS configuration information and status.

aps direction

To specify unidirectional or bidirectional path switching, use the **aps direction** command. To revert to the default behavior, use the **no** form of this command.

   aps direction {**unidirectional** | **bidirectional**}

   no aps direction

Syntax Description

unidirectional	Specifies unidirectional path switching.
bidirectional	Specifies bidirectional path switching.

Defaults   Unidirectional

Command Modes   APS configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   In unidirectional path switching, only the node that detects a signal failure switches over. The other node continues to receive its signal on the original path. In bidirectional path switching, when a node detects a signal failure it sends a message to the other node about the failure causing that node to switch over. Both nodes then use the same path through the network.

Use the **aps direction** command only with splitter and y-cable line card protection configurations. Client line card protection handles switchovers in the client equipment, not in the Cisco ONS 15540 ESPx.

When using bidirectional path switching, always configure the nodes so that they communicate over the same working path and the same protection path. Also, configure both nodes that support the channel with the same APS features, such as y-cable support, revertive behavior, and path switching.

Before changing the type of path switching, disable the standby interface with the **shutdown** command. After changing the type of path switching, reenable the standby interface with the **no shutdown** command

Note Bidirectional path switching only operates on networks that support the OSC.

Note Configure bidirectional path switching on interfaces configured with Sysplex ETR or Sysplex CLO protocol encapsulation.

Examples The following example shows how to configure bidirectional path switching for a 2.5G interface in a y-cable protection configuration.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group alpha
Switch(config-red-aps)# working transparent 2/0/0
Switch(config-red-aps)# protection transparent 4/0/0
Switch(config-red-aps)# aps y-cable
Switch(config-red-aps)# aps direction bidirectional
Switch(config-red-aps)# aps enable
```

The following example shows how to configure bidirectional path switching for a 10-GE interface in a y-cable protection configuration.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group alpha
Switch(config-red-aps)# working tengigethernetphy 2/0
Switch(config-red-aps)# protection tengigethernetphy 4/0
Switch(config-red-aps)# aps y-cable
Switch(config-red-aps)# aps direction bidirectional
Switch(config-red-aps)# aps enable
```

The following example shows how to configure bidirectional path switching in a splitter protection configuration.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group chicago
Switch(config-red-aps)# working wavepatch 10/2/0
Switch(config-red-aps)# protection wavepatch 10/2/1
Switch(config-red-aps)# aps direction bidirectional
Switch(config-red-aps)# aps enable
```

The following example shows how to change the path switching operation for a y-cable APS group from unidirectional to bidirectional.

```
Switch# show aps group alpha

APS Group alpha :

  architecture.: 1+1, remote prov: 1+1
  span.........: end-to-end (client side y-cable)
  direction....: prov: uni, current: uni, remote prov: bi
  revertive....: no
  created......: 14 hours, 53 minutes
  aps state....: associated (enabled)
  request timer: holddown: 5000 ms, max: 15000 ms, count 2
  switched chan: 0
→ channel  ( 0): Transparent4/3/0 (STANDBY - UP), Wave4/3 (UP)
                : channel  request: no-request
```

```
                     : transmit request: no-request
                     : receive  request: no-request
     channel  ( 1): Transparent2/3/0 (ACTIVE - UP), Wave2/3 (UP)
                     : channel  request: no-request
                     : switchover count: 0
                     : last  switchover: never

Switch# configure terminal
Switch(config)# interface transparent 4/3/0
Switch(config-if)# shutdown
Switch(config-if)# exit
Switch(config)# redundancy
Switch(config-red)# associate group Denver
Switch(config-red-aps)# aps disable
Switch(config-red-aps)# aps direction bidirectional
Switch(config-red-aps)# aps enable
Switch(config-red-aps)# exit
Switch(config-red)# exit
Switch(config)# interface transparent 4/3/0
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch#
```

Related Commands

Command	Description
aps disable	Disables APS activity between associated interfaces.
aps enable	Enables APS activity between associated interfaces.
aps revertive	Configures revertive APS for y-cable line card protection.
aps timer message holddown	Modifies the APS channel protocol message holddown timer interval and message count value.
aps timer message max-interval	Modifies the APS channel protocol maximum inactivity interval timer value.
aps timer search-for-up	Modifies the minimum and maximum timer intervals on an APS timer that the system must wait for a splitter protection connection to come up when both connections are down.
aps timer switchover-enable min-interval	Modifies the minimum timer interval before reenabling APS switchover.
aps timer wait-to-restore	Modifies the number of seconds an APS timer must wait before switching back to the preferred working signal.
aps working	Configures the working interface of an associated interface pair.
aps y-cable	Enables y-cable protection.
associate group	Creates an APS group and enters APS configuration mode.
associate interface	Associates multiple wavepatch interface pairs for APS protection.
show aps	Displays APS configuration information and status.

aps disable

To disable APS activity between an associated interface pair, use the **aps disable** command. To reenable APS activity, use the **aps enable** command.

aps disable

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   APS configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Before changing the APS configuration of an associated interface pair, use this command to disable APS activity between the interfaces. When an interface pair is initially associated, APS activity is disabled.

Examples   The following example shows how to disable APS activity between associated transparent interfaces.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group newyork
Switch(config-red-aps)# aps disable
```

Related Commands

Command	Description
aps enable	Enables APS activity between associated interfaces.
associate group	Creates an APS group and enters APS configuration mode.

Cisco ONS 15540 ESPx Command Reference Guide

aps enable

To enable APS activity between an associated interface pair, use the **aps enable** command. To disable APS activity, use the **aps disable** command.

aps enable

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   APS configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   After changing the APS configuration of an associated interface pair, use this command to enable APS activity between the interfaces.

Examples   The following example shows how to enable APS activity between associated transparent interfaces.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group london
Switch(config-red-aps)# aps working transparent 2/0/0
Switch(config-red-aps)# aps protection transparent 4/0/0
Switch(config-red-aps)# aps enable
```

Related Commands	Command	Description
	aps disable	Disables APS activity between associated interfaces.
	associate group	Creates an APS group and enters APS configuration mode.

aps lockout

To lock out an APS switchover to the protection path, thus preventing any further APS switchovers for any reason, including manual or forced switchovers and signal failures, use the **aps lockout** command. To remove an APS lockout request, use the **aps clear** command.

> **aps lockout** *group-name*

Syntax Description   This command has no other arguments or keywords.

Defaults   Disabled

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to configure APS signal switchover lockout on the protection path. This is useful when you want to prevent a switchover during shelf maintenance, or when the protection signal has degraded or failed.

A lockout only succeeds when the protection path interface is also acting as the standby interface. If the protection path interface is the active interface, use the **aps switch** command to switch the active interface role back to the working interface.

Note   The APS lockout does not persist across system reloads or processor card switchovers.

Examples   The following example shows how to lock out switchover to the protection path on an associated group named group1.

```
Switch# aps lockout group1
```

Related Commands	Command	Description
	aps clear	Clears the APS switchover or lockout.
	aps switch	Requests an APS switchover.
	aps working	Configures the working interface of an associated interface pair.
	show aps	Displays APS configuration information and status.

aps message-channel

To configure message channel to send APS channel protocol messages for the Cisco ONS 15540 ESPx, use the **aps message-channel** command. To revert to the default behavior, use the **no** form of this command.

> **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*]}

> **no aps message-channel**

Syntax Description

auto-select	APS automatically selects a transport mechanism to send APS messages.
far-end group-name *name*	Specifies the APS group name for the channel at the remote node.
inband dcc	Specifies APS to use the in-band message channel for sending APS messages.
ip	Specifies APS messages are sent over IP. APS addresses the messages to a specified group name on the remote node identified by this IP address.
ip-address *ip-address*	Specifies the IP address to use to send the APS channel protocol messages.
osc	APS messages are sent on the OSC.

Defaults   auto-select

Command Modes   APS configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   The APS channel protocol communicates between nodes over the OSC or over the in-band message channel ethernetdcc interface.

The **auto-select** option automatically selects the transport channel to send the APS protocol messages attempting to use the in-band message channel first and then the OSC if the in-band message channel is not available. If neither the in-band message channel nor the OSC is available for the APS group, you must configure the message channel using the **ip** option.

> **Note**   We recommend that you configure the name for the APS group on the remote node. The APS channel protocol lookup process functions more efficiently when the group name is provided. For trunk fiber based protection, the far-end group name is required.

Examples   The following example shows how to create an APS group and configure the message channel.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group aps_group
Switch(config-red-aps)# aps message-channel osc
```

Related Commands

Command	Description
aps lockout	Prevents switchover to the protection path.
aps working	Configures the working interface for an APS interface pair.
aps y-cable	Enables y-cable protection.
associate group	Creates an APS group and enters APS configuration mode.
associate interface	Associates multiple wavepatch interface pairs for APS protection.
show aps	Displays APS configuration and operation information.

aps protection

To configure the protection path interface of an APS group, use the **aps protection** command. To remove the protection path interface, use the **no** form of this command.

> **aps protection** {**transparent** *slot/subcard/port* | **wavepatch** *slot/subcard/port* | *tengigethernetphy slot/subcard* | **wdmsplit** *slot/subcard/port*}

> **no aps protection** {**transparent** *slot/subcard/port* | **wavepatch** *slot/subcard/port* | *tengigethernetphy slot/subcard* | **wdmsplit** *slot/subcard/port*}

Syntax Description

transparent *slot/subcard/port*	Specifies the transparent interface to use as the protection path in y-cable line card protection.
wavepatch *slot/subcard/port*	Specifies the wavepatch interface to use as the protection path in splitter protection.
tengigethernetphy slot/subcard	Specifies the tengigethernetphy interface to use as the protection path in splitter protection.
wdmsplit *slot/subcard/port*	Specifies the wdmsplit interface to use as the protection path in trunk fiber based protection.

Defaults   None

Command Modes   APS configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
12.1(10)EV2	Support for 10-GE transponder module was added.
12.1(12c)EV	Support for wdmsplit interfaces and trunk fiber based protection was added.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Each interface in an associated pair has a configured role to perform: one is the *working* interface and the other is the *protection* interface. However, at any given instant, the interfaces also have a current mode of operation: *active* and *standby*. The interface that is in active mode and receives the signal may or may not be the working interface. The working interface is the *preferred* interface to receive the active signal. The protection interface is the *preferred* interface for the standby signal.

When a pair of interfaces is associated for APS protection using the **associate interface** command, the interface with the higher interface number is the protection interface by default. To override this default configuration, use the **aps protection** command.

Examples   The following example shows how to create an APS group and configure an APS protection interface.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group denver
Switch(config-red-aps)# aps working transparent 2/0/0
Switch(config-red-aps)# aps protection transparent 4/0/0
Switch(config-red-aps)# aps enable
```

Related Commands

Command	Description
aps lockout	Prevents switchover to the protection path.
aps working	Configures the working interface for an APS interface pair.
aps y-cable	Enables y-cable protection.
associate group	Creates an APS group and enters APS configuration mode.
associate interface	Associates multiple wavepatch interface pairs for APS protection.
show aps	Displays APS configuration and operation information.

aps revertive

To configure revertive APS for y-cable line card protection, use the **aps revertive** command. To disable revertive APS, use the **no** form of this command.

aps revertive

no aps revertive

Syntax Description   This command has no other arguments or keywords.

Defaults   Disabled

Command Modes   APS configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   When revertive APS is configured and a switchover to the protection signal has occurred, the system automatically switches back to the preferred working signal when it becomes operational. Use the **aps timer wait-to-restore** command to control how quickly the signal reverts back to the working path.

Note   Revertive APS is only supported with y-cable line card protection.

Examples   The following example shows how to configure revertive APS on an associated transparent interface pair.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group dallas
Switch(config-red-aps)# aps working transparent 2/0/0
Switch(config-red-aps)# aps protection transparent 4/0/0
Switch(config-red-aps)# aps revertive
```

```
Switch(config-red-aps)# aps y-cable
Switch(config-red-aps)# aps enable
```

Related Commands	Command	Description
	aps disable	Disables APS activity between associated interfaces.
	aps enable	Enables APS activity between associated interfaces.
	aps timer switchover-enable min-interval	Modifies the minimum timer interval before reenabling APS switchover.
	aps timer wait-to-restore	Modifies the wait-to-restore timer interval.
	associate group	Creates an APS group and enters APS configuration mode.
	show aps	Displays APS configuration and operation information.

aps switch

To request an APS switchover from the working path to the protection path, or from the protection path to the working path, use the **aps switch** command. To clear an APS switchover request, use the **aps clear** command.

aps switch *group-name* {**force** | **manual**} {**protection-to-working** | **working-to-protection**}

Syntax Description	group-name	Specifies the name of the associated pair of interfaces.
	force	Causes a switchover if no lockout is in effect.
	manual	Causes a switchover if the signal is good and no lockout is in effect.
	protection-to-working	Causes a manual signal switchover from the protection path to the working path if the protection path signal has not failed.
	working-to-protection	Causes a manual signal switchover from the working path to the protection path whether the working path signal is active or not.

Defaults   None

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   The Cisco ONS 15540 ESPx supports APS switchover requests from the CLI (command-line interface). These requests have priorities depending on the condition of the protection signal and the existence of other switchover requests. There are three types of requests:

- Lockout requests—Have the highest priority and take effect regardless of the condition of the protection signal. A lockout prevents the signal from switching over from the working interface to the protection interface.

- Forced switchover requests—Have the next highest priority and are only prevented if there is an existing lockout on the protection interface, or the protection signal has failed.

- Manual switchover requests—Have the lowest priority and only occur if there is no protection interface lockout, a forced switchover, or the signal has failed or degraded.

In summary, the priority order is:

1. Lockout
2. Signal failure on the protection path
3. Forced signal switchover
4. Signal failure on the working path
5. Signal degrade on the working or protection path
6. Manual signal switchover

If a request or condition of a higher priority is in effect, a lower priority request is rejected.

Note The associated group names are case sensitive and must be entered exactly as they are shown in the **show aps** command output.

Examples   The following example shows how to make a manual switchover request from the working path to the protection path for an associated interface pair named blue.

```
Switch# aps switch blue manual working-to-protection
```

The following example shows how to make a force switchover request from the working to the protection path for an associated interface pair with the default group name.

```
Switch# aps switch Wavepatch2/0/0 force protection-to-working
```

Related Commands

Command	Description
aps clear	Clears APS switchover or lockout.
aps lockout	Prevents switchover to the protection interface.
associate group	Creates an APS group and enters APS configuration mode.
associate interface	Associates multiple wavepatch interface pairs for APS protection.
show aps	Displays APS configuration and operation information.

aps timer message holddown

To modify the APS channel protocol holddown timer, use the **aps timer message holddown** command. To revert to the default values, use the **no** form of this command.

> **aps timer message holddown** *milliseconds* [**count** *number*]

> **no aps timer message holddown**

Syntax Description

milliseconds	Specifies the number of seconds to wait before sending an APS channel protocol message. The range is 100 to 10,000 milliseconds. The default timer interval is 5000 milliseconds (5 seconds).
count *number*	Specifies the number of messages to send to the destination node before starting the hold-down timer. The range is 2 to 10. The default message count is 2.

Defaults   See the "Syntax Description" section.

Command Modes   APS configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   The holddown timer prevents APS channel protocol message flooding over the OSC. The holddown message count allows a specified number of messages to exchange between the nodes before the holddown timer starts. For example, if the holddown message count is set to 2, the node sends and receives two messages before the timer starts. This allows the protocol to operate efficiently without affecting system performance.

✎
Note   The default values for the holddown timer and message count are sufficient for most network configurations.

Examples   The following example shows how to modify the holddown timer and count values.

```
Switch(config)# redundancy
Switch(config-red)# associate group denver
Switch(config-red-aps)# aps disable
Switch(config-red-aps)# aps timer message holddown 4000 count 4
Switch(config-red-aps)# aps enable
```

Related Commands

Command	Description
aps disable	Disables APS activity between associated interfaces.
aps enable	Enables APS activity between associated interfaces.
aps timer message max-interval	Modifies the APS channel protocol maximum interval timer value.
associate group	Creates an APS group and enters APS configuration mode.
associate interface	Associates multiple wavepatch interface pairs for APS protection.
show aps	Displays APS configuration and operation information.

aps timer message max-interval

To modify the maximum interval for the APS channel protocol inactivity timer, use the **aps timer message max-interval** command. To revert to the default value, use the **no** form of this command.

aps timer message max-interval *seconds*

no aps timer message max-interval

Syntax Description	seconds	Specifies the maximum number of seconds to wait before sending an APS channel protocol inactivity message. The range is 1 to 120 seconds.

Defaults   15 seconds

Command Modes   APS configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   To ensure that the APS channel protocol is still functioning between the nodes, periodic messages are sent during periods of inactivity. The maximum interval of the inactivity timer determines how often to send the inactivity messages.

> **Note**   The default value for the inactivity timer maximum interval is sufficient for most network configurations.

Examples   The following example shows how to modify the maximum interval for the inactivity timer.

```
Switch(config)# redundancy
Switch(config-red)# associate group dallas
Switch(config-red-aps)# aps disable
```

```
Switch(config-red-aps)# aps timer message max-interval 30
Switch(config-red-aps)# aps enable
```

Related Commands	Command	Description
	aps disable	Disables APS activity between associated interfaces.
	aps enable	Enables APS activity between associated interfaces.
	aps timer message holddown	Modifies the APS channel protocol holddown timer and message count values.
	associate group	Creates an APS group and enters APS configuration mode.
	associate interface	Associates multiple wavepatch interface pairs for APS protection.
	show aps	Displays APS configuration and operation information.

aps timer search-for-up

To modify the minimum and maximum timer intervals on an APS timer for the length of time the system waits for a splitter protection connection to come up when both connections are down, use the **aps timer search-for-up** command. To revert to the default values, use the **no** form of this command.

aps timer search-for-up *min-interval max-interval*

no aps timer search-for-up

Syntax Description

min-interval	Specifies the minimum time interval to wait for a splitter protection connection to come up before checking the other signal. The range is 1 to 120 seconds.
max-interval	Specifies the maximum timer interval to wait for a splitter protection connection to come up before checking the other signal. The range is 1 to 120 seconds.

Defaults

Minimum interval: 2 seconds

Maximum interval: 32 seconds

Command Modes

APS configuration

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to modify the minimum and maximum timer intervals on an APS timer that causes the system to wait for a splitter protection connection to come up before checking the other splitter protection connection.

When both members of a splitter pair are down, the system first checks one signal for the minimum time interval. If the splitter protection connection does not come up, the system checks the other connection and doubles the time interval. This process repeats until the maximum timer interval is reached or exceeded. Checking continues at the maximum timer interval until one of the splitter protection connections becomes active.

Note   The default values for the search-for-up timer are sufficient for most network configurations.

Examples   The following example shows how to modify the minimum and maximum timer intervals for how often the system switches to check the other splitter protection connection.

```
Switch(config)# redundancy
Switch(config-red)# associate group newyork
Switch(config-red-aps)# aps disable
Switch(config-red-aps)# aps timer search-for-up 4 16
Switch(config-red-aps)# aps enable
```

Related Commands

Command	Description
aps disable	Disables APS activity between associated interfaces.
aps enable	Enables APS activity between associated interfaces.
aps timer switchover-enable min-interval	Modifies the minimum timer interval before reenabling APS switchover.
associate group	Creates an APS group and enters APS configuration mode.
associate interface	Associates multiple wavepatch interface pairs for APS protection.
show aps	Displays APS configuration and operation information.

aps timer switchover-enable min-interval

To modify the minimum time interval between successive APS switchovers, use the **aps timer switchover-enable min-interval** command. To revert to the default value, use the **no** form of this command.

aps timer switchover min-interval *seconds*

no aps timer switchover-enable min-interval

Syntax Description

seconds	Specifies the minimum number of seconds between successive switchovers. The range is 1 to 120 seconds.

Defaults   3 seconds

Command Modes   APS configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
12.1(12c)EV2	Default value changed from 2 seconds to 3 seconds.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Hardware-assisted automatic switchovers when the active signal fails are controlled by the software. An automatic switchover occurs when the system detects a signal failure or signal degradation. Automatic switchovers are disabled until the switchover timer expires. The switchover timer starts upon completion of the automatic switchover. When the timer expires, the system will allow automatic switchovers only under favorable conditions. Conditions that would prevent the system from enabling automatic switchovers include:

- Loss of Light on the protection signal
- Lockout request on the protection interface, either locally or on the remote system supporting the channel

- Forced protection-to-working request in effect, either locally or on the remote system supporting the channel

- Poor quality of the protection signal

When the condition is resolved, hardware-assisted automatic switchovers are enabled.

The switchover timer prevents successive automatic switchovers from occurring too quickly and risk the loss of data.

Note   The default value for the switchover timer is sufficient for most network configurations.

Examples   The following example shows how to modify the minimum interval between successive signal switchovers.

```
Switch(config)# redundancy
Switch(config-red)# associate group sanfrancisco
Switch(config-red-aps)# aps disable
Switch(config-red-aps)# aps timer switchover-enable min-interval 4
Switch(config-red-aps)# aps enable
```

Related Commands

Command	Description
aps disable	Disables APS activity between associated interfaces.
aps enable	Enables APS activity between associated interfaces.
aps timer wait-to-restore	Modifies the wait-to-restore timer interval.
associate group	Creates an APS group and enters APS configuration mode.
show aps	Displays APS configuration and operation information.

aps timer wait-to-restore

To modify the number of seconds on the APS wait-to-restore timer before reverting to the preferred working signal in a y-cable protection configuration, use the **aps timer wait-to-restore** command. To return to the default value, use the **no** form of this command.

aps timer wait-to-restore *seconds*

no aps timer wait-to-restore

Syntax Description

seconds	Specifies the number of seconds the system must wait before switching to the preferred working signal. The range is 0 to 720 seconds.

Defaults   300 seconds

Command Modes   APS configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   This command prevents oscillations when revertive switching is configured for y-cable line card protection configurations. If the preferred working signal in a y-cable line card protection configuration is unstable, the wait-to-restore timer prevents possible data loss that could result from frequent switchovers.

⚠

Caution   Setting the wait-to-restore timer interval to 0 seconds disables the timer.

✎

Note   The wait-to-restore timer is only supported in y-cable line card protection configurations.

> **Note** The default value for the wait-to-restore timer is sufficient for most network configurations.

Examples The following example shows how to modify the APS wait-to-restore timer.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group newyork
Switch(config-red-aps)# aps disable
Switch(config-red-aps)# aps timer wait-to-restore 180
Switch(config-red-aps)# aps enable
```

Related Commands

Command	Description
aps disable	Disables APS activity between associated interfaces.
aps enable	Enables APS activity between associated interfaces.
aps revertive	Enables revertive behavior for line card protection.
aps timer switchover-enable min-interval	Modifies the minimum timer interval before reenabling APS switchover.
associate group	Creates an APS group and enters APS configuration mode.
show aps	Displays APS configuration and operation information.

aps working

To configure the working interface of an APS group, use the **aps working** command. To remove the working interface, use the **no** form of this command.

>aps working {**transparent** *slot*/*subcard*/*port* | **wavepatch** *slot*/*subcard*/*port*
> |*tengigethernetphy slot*/*subcard* | **wdmsplit** *slot*/*subcard*/*port*}

>no aps working {**transparent** *slot*/*subcard*/*port* | **wavepatch** *slot*/*subcard*/*port* |
>   *tengigethernetphy slot*/*subcard* | **wdmsplit** *slot*/*subcard*/*port*}

Syntax Description

transparent *slot*/*subcard*/*port*	Specifies the transparent interface to use as the working interface in y-cable line card protection.
wavepatch *slot*/*subcard*/*port*	Specifies the wavepatch interface to use as the working interface in splitter protection.
tengigethernetphy slot/*subcard*	Specifies the tengigethernetphy interface to use as the working interface in splitter protection.
wdmsplit *slot*/*subcard*/*port*	Specifies the wdmsplit interface to use as the working path in trunk fiber based protection.

Defaults   None

Command Modes   APS configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
12.1(10)EV2	Support for 10-GE transponder module was added.
12.1(12c)EV	Support for wdmsplit interfaces and trunk fiber based protection was added.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Each interface in an associated pair has a configured role to perform: one is the *working* interface and the other is the *protection* interface. However, at any given instant, the interfaces also have a current mode of operation: *active* and *standby.* The interface that is in active mode, and is receiving the signal, may or may not be the working interface. The working interface is the *preferred* interface to receive the active signal. The protection interface is the *preferred* interface for the standby signal.

This command persists across system reloads.

When a pair of interfaces is associated for APS protection, the interface with the lower interface number is the working interface by default. To override this default configuration, use the **aps working** command. If there is an **aps lockout** command in effect on the protection interface, it cannot become the working interface.

Examples   The following example shows how to configure a working interface on an existing APS group.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate group denver
Switch(config-red-aps)# aps disable
Switch(config-red-aps)# aps working transparent 4/0/0
Switch(config-red-aps)# aps protection transparent 2/0/0
Switch(config-red-aps)# aps enable
```

Related Commands

Command	Description
aps lockout	Prevents switchover to the protection interface.
aps y-cable	Enables y-cable protection.
associate group	Creates an APS group and enters APS configuration mode.
associate interface	Associates multiple wavepatch interface pairs for APS protection.
show aps	Displays APS configuration and operation information.

aps y-cable

To configure y-cable line card protection, use the **aps y-cable** command. To disable y-cable line card protection, use the **no** form of this command.

aps y-cable

no aps y-cable

Syntax Description   This command has no other arguments or keywords.

Defaults   Disabled

Command Modes   APS configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
12.1(10)EV2	Support for 10-GE transponder module was added.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to ensure that only one interface of an associated transparent or tengigethernetphy interface pair transmits to the client. Signal corruption occurs when both interfaces in the pair transmit to the client over the y-cable.

⚠

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

Examples   The following example shows how to configure y-cable line card protection.

```
Switch(config)# redundancy
Switch(config-red)# associate group seattle
Switch(config-red-aps)# aps disable
```

```
Switch(config-red-aps)# aps y-cable
Switch(config-red-aps)# aps enable
```

Related Commands	Command	Description
	aps direction	Modifies path switching behavior.
	aps disable	Disables APS activity between associated interfaces.
	aps enable	Enables APS activity between associated interfaces.
	aps revertive	Enables revertive behavior for line card protection.
	aps timer switchover-enable min-interval	Modifies the minimum timer interval before reenabling APS switchover.
	aps timer wait-to-restore	Modifies the wait-to-restore timer interval.
	associate group	Creates or specifies an APS interface group and enters APS configuration mode.
	show aps	Displays APS configuration and operation information.

associate group

To enter APS configuration subcommand mode and to associate interfaces for APS protection, or to modify the attributes of an existing APS group, use the **associate group** command. To remove the group, use the **no** form of this command.

aps group *group-name*

no aps group *group-name*

Syntax Description

group-name	Specifies a group name for the interface pair. Group names are case sensitive and cannot have embedded blanks.

Defaults   None

Command Modes   Redundancy configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to create an APS group, or specify an existing group, and enter APS configuration mode. You can specify group names created with this command or with the **associate interface** command.

Examples   The following example shows how to select an APS group and enter APS configuration mode.

```
Switch# configure terminal
Switch#(config)# redundancy
Switch#(config-red)# associate group blue
Switch#(config-red-aps)#
```

	Command	Description
Related Commands	**aps clear**	Clears APS switchover or lockout.
	aps direction	Modifies path switching behavior.
	aps disable	Disables APS activity between associated interfaces.
	aps enable	Enables APS activity between associated interfaces.
	aps lockout	Prevents switchover to the protection interface.
	aps revertive	Enables revertive behavior for line card protection.
	aps switch	Requests an APS switchover.
	aps timer message holddown	Modifies the hold-down timer for APS channel protocol messages.
	aps timer message max-interval	Modifies the maximum interval timer for APS channel protocol messages.
	aps timer search-for-up	Modifies the search-for-up timer interval.
	aps timer switchover-enable min-interval	Modifies the minimum timer interval before reenabling APS switchover.
	aps timer wait-to-restore	Modifies the wait-to-restore timer interval.
	aps working	Configures the working interface of an associated interface pair.
	aps y-cable	Enables y-cable protection.
	associate interface	Associates wavepatch interfaces for APS splitter protection.
	debug aps	Enables debugging of APS and APS channel protocol.
	redundancy	Enters redundancy configuration mode.
	show aps	Displays APS configuration and operation information.
	show aps trace	Displays APS and APS channel protocol activity information.
	snmp-server enable traps aps	Enables SNMP trap notifications for APS.

associate interface

To associate the wavepatch interface pairs in a slot, or in the entire shelf, for APS splitter protection using one command, use the **associate interface** command. To disable APS protection for the interfaces, use the **no** form of this command.

associate interface wavepatch */*/*working-port* **wavepatch** */*/*protection-port* [**enable** | **disable**]

associate interface wavepatch *slot/*/*working-port* **wavepatch** *slot/*/*protection-port* [**enable** | **disable**]

no associate interface wavepatch */*/*working-port* **wavepatch** */*/*protection-port*

no associate interface wavepatch *slot/*/*working-port* **wavepatch** *slot/*/*protection-port*

Syntax Description

wavepatch */*/*working-port*	Specifies all wavepatch interfaces on the shelf to configure as working interfaces.
wavepatch */*/*protection-port*	Specifies all wavepatch interfaces in the shelf to configure as protection interfaces.
enable	Enables activity on the associated interface pairs. (Optional)
disable	Disables activity on the associated interface pairs. This is the default state. (Optional)
wavepatch *slot/*/*working-port*	Specifies all wavepatch interfaces in a slot to configure as working interfaces.
wavepatch *slot/*/*protection-port*	Specifies all wavepatch interfaces in a slot to configure as protection interfaces.

Defaults

The default working interface for each of the interface pairs is the first interface in the command.

APS activity between the interfaces is disabled when the interface pairs are first associated.

The default group name for each of the interface pairs is the lower interface number.

Command Modes

Redundancy configuration

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to associate the interfaces for APS protection, and then enter APS configuration mode, or to change the configuration of associated pairs. Also use this command to change the association of one interface to another interface.

When associating wavepatch interfaces with wildcards, the command mode does not enter APS configuration mode as it does when associating a pair of interfaces. Changes to the default APS attribute values must be entered for interface pairs individually. See the "Examples" section.

Associating wavepatch interfaces with wildcards does not overwrite attributes configured for a specific interface pair. For example, if you configure attributes for interface pair wavepatch 3/0/0 and wavepatch 3/0/1 with the **associate group** command, a subsequent **associate interface wavepatch 3/*/0 wavepatch 3/*/1** command does not change the attributes for the specific interface pair.

When a pair of interfaces is associated for APS protection with the **associate interface** command, the interface entered first in the command is the working interface by default.

Interfaces can be associated without being physically present in the shelf.

Examples

The following example shows how to associate all the wavepatch interfaces in the shelf for splitter protection while leaving APS activity between the interfaces disabled.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate interface wavepatch */*/0 wavepatch */*/1
Switch(config-red)#
```

The following example shows how to associate all the wavepatch interfaces in slot 2 for splitter protection, while enabling APS activity between the interfaces.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# associate interface wavepatch 2/*/0 wavepatch 2/*/1 enable
Switch(config-red)#
```

Related Commands

Command	Description
aps clear	Clears APS switchover or lockout.
aps direction	Modifies path switching behavior.
aps disable	Disables APS activity between associated interfaces.
aps enable	Enables APS activity between associated interfaces.
aps lockout	Prevents switchover to the protection interface.
aps switch	Requests an APS switchover.
aps timer message holddown	Modifies the hold-down timer for APS channel protocol messages.
aps timer message max-interval	Modifies the maximum interval timer for APS channel protocol messages.
aps timer search-for-up	Modifies the search-for-up timer interval.
aps working	Configures the working interface of an associated interface pair.

Command	Description
associate group	Creates or specifies an APS interface group and enters APS configuration mode.
debug aps	Enables debugging of APS and APS channel protocol.
redundancy	Enters redundancy configuration mode.
show aps	Displays APS configuration and operation information.
show aps trace	Displays APS and APS channel protocol activity information.
snmp-server enable traps aps	Enables SNMP trap notifications for APS.

show aps

To display APS configuration and status information for the system, use the **show aps** command.

show aps [detail | group *name* | interface *interface*]

Syntax Description

detail	Displays detailed APS information for all APS groups.
interface *interface*	Displays detailed APS information for an interface.
group *name*	Displays detailed APS information for an APS group.

Defaults   Displays summary APS information

Command Modes   EXEC and privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to display APS information for an interface, an APS group, or the entire shelf.

At least one interface in an associated pair must be present on the system to use the **show aps interface** command. Otherwise, use the **show aps detail** command or the **show aps group** command to display APS information for the associated interface pair.

Note   The associated group names are case sensitive. To see all the group names, use the **show aps** command.

Examples   The following example shows how to display detailed APS information for all APS groups. (See Table 1-1 for field descriptions.)

```
Switch# show aps detail

APS Group blue:
```

Cisco ONS 15540 ESPx Command Reference Guide

```
architecture.: 1+1, remote prov: 1+1
span.........: end-to-end (client side y-cable)
direction....: prov: uni, current: uni, remote prov: uni
revertive....: yes, wtr: 60 secs (not running)
created......: 4 minutes
aps state....: associated (enabled)
request timer: holddown: 5000 ms, max: 15000 secs, count 2
switched chan: 0
channel  ( 0): Transparent5/0/0 (STANDBY - UP), Wave5/0 (UP)
             : channel  request: no-request
             : transmit request: no-request
             : receive  request: no-request
channel  ( 1): Transparent3/0/0 (ACTIVE - UP), Wave3/0 (UP)
             : channel  request: no-request
             : switchover count: 0
             : last  switchover: never
```

Table 1-1   show aps group and show aps interface Field Descriptions

Field	Description
architecture	Shows APS architecture. Only 1+1 is supported.
remote prov:	Shows the architecture provisioning for the remote node that supports the same channel. Only 1+1 is supported.
span	Shows the APS span. Only end-to-end is supported. Also indicates if y-cable is configured.
direction	Shows signal switching behavior, either unidirectional or bidirectional.
prov:	Shows the direction provisioning for the local node.
current:	Shows the current direction status for the local node.
remote prov:	Shows the direction provisioning for the remote node that supports the same channel.
revertive	Indicates whether the group is APS revertive. Only y-cable line card protection supports revertive behavior.
wtr:	Shows the wait-to-restore timer value and its current running status.
created	Shows how long ago the group was created.
aps state	Indicates whether the working and protection channels have been associated and if APS activity is enabled.
request timer	Shows attribute values for the APS channel protocol timers.
holddown:	Shows the APS channel protocol message holddown timer value.
max:	Shows the APS channel protocol maximum inactivity interval timer.
count:	Shows the APS channel protocol message count value.
switched chan:	Shows the switched channel number.
channel (0)	Shows the configured protection channel in the group and its current status.

Table 1-1   show aps group and show aps interface Field Descriptions (continued)

Field	Description
channel request:	Shows the current lockout or switchover request in effect, if any. Valid values are: • no-request • manual-switch • forced-switch • lockout-of-protection
transmit request:	Shows the APS channel protocol message being transmitted to the remote node.Valid values are: • no-request (No request pending) • do-not-revert (Revertive behavior not enabled) • reverse-request (Response to a do-not-revert or wait-to-restore request) • wait-to-restore (Wait-to-restore timer active) • sd-lp (Signal degrade) • sf-lp (Signal failure)
receive request:	Shows the APS channel protocol message being received from the remote node. Values are the same as the transmit request field.
channel (1)	Shows the configured working channel in the group and its current status.
switchover count:	Shows the number of times a switchover as occurred for this pair of interfaces. Zero (0) indicates that no switchover has occurred since the system was booted.
last switchover:	Shows the elapsed time since the last switchover occurred. "Never" means that no switchover has occurred since the system was booted.

The following example shows how to display APS information for an APS group with the default group name (the default working interface). (See Table 1-1 for field descriptions.)

```
Switch# show aps group Wavepatch8/0/0

APS Group Wavepatch8/0/0 :

  architecture.: 1+1, remote prov: 1+1
  span.........: end-to-end (network side splitter)
  direction....: prov: bi, current: bi, remote prov: bi
  revertive....: no
  created......: 3 hours, 6 minutes
  aps state....: associated (enabled)
  request timer: holddown: 5000 ms, max: 15000 ms, count 2
  search-up int: min: 2 secs, max: 32 secs
  switched chan: 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: 1
               : last  switchover: 1 hour, 0 minutes
```

The following example shows how to display APS information for a wavepatch interface. (See Table 1-1 for field descriptions.)

```
Switch# show aps interface transparent 8/0/0

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
  created......: 1 minute
  aps state....: associated (enabled)
  request timer: holddown: 5000 ms, max: 15000 ms, count 2
  switched chan: 0
  channel  ( 0): Transparent10/0/0 (STANDBY - UP)
               : external request: no-request
               : transmit request: no-request
               : receive  request: no-request
  channel  ( 1): Transparent8/0/0 (STANDBY - UP)
               : external request: no-request
               : switchover count: 0
               : last switchover.: never
```

The following example shows how to display APS summary information. (See Table 1-2 for field descriptions.)

```
Switch# show aps

AR :APS Role, Wk:Working, Pr:Protection
AS :APS State, Ac:Active, St:Standby
IS :Interface State, Up:Up, Dn:Down
MPL:Minimum Protection Level, SD:Signal Degrade, SF:Signal Failure
    LOL:Loss of Light, - not currently protected

Interface        AR AS IS MPL Redundant Intf    Group Name
~~~~~~~~~~~~~~~~~ ~~ ~~ ~~ ~~~ ~~~~~~~~~~~~~~~~~ ~~~~~~~~~~~~~~~~~~~~
Wavepatch3/1/0    Wk Ac Up LOL Wavepatch3/1/1   Wavepatch3/1/0
Wavepatch3/1/1    Pr St Up LOL Wavepatch3/1/0   Wavepatch3/1/0
```

Table 1-2   show aps summary Field Descriptions

Field	Description
Interface	Shows the name of the interface.
AR (APS Role)	Shows the configured role for the interface, either Wk (working) or Pr (protection). Working and protection are preferred roles configured by the **associate interface** command and the **associate group** command.
AS (APS State)	Shows the APS state, either Ac (active) or St (standby). The interface currently chosen by the system to receive the channel signal is the active interface; the other interface in the associated pair is the standby.
IS (Interface State)	Shows the interface state, either Up (up) or Dn (down).

Table 1-2   show aps summary Field Descriptions (continued)

Field	Description
MPL (Minimum Protection Level)	Shows the minimum protection level for signal switchover. Valid values are: • SD (signal degrade) • SF (signal failure) • LOL (loss of light) • - (not currently protected)
Redundant Intf (Interface)	Shows the other interface in the APS group.
Group Name	Shows the APS group name for the interface.

Related Commands

Command	Description
aps direction	Specifies unidirectional or bidirectional path switching.
aps disable	Disables APS activity between associated interfaces.
aps enable	Enables APS activity between associated interfaces.
aps lockout	Configures APS lockout on a protection interface.
aps revertive	Configures revertive APS for y-cable line card protection.
aps switch	Causes a manual switchover from the working interface to the protection interface or vice versa.
aps timer message holddown	Modifies the APS channel protocol message holddown timer interval and message count value.
aps timer message max-interval	Modifies the APS channel protocol maximum inactivity interval timer value.
aps timer search-for-up	Modifies the minimum and maximum timer intervals on an APS timer that the system must wait for a splitter protection connection to come up when both connections are down.
aps timer switchover-enable min-interval	Modifies the minimum timer interval before reenabling APS switchover.
aps timer wait-to-restore	Modifies the number of seconds an APS timer must wait before switching back to the preferred working signal.
aps working	Explicitly configures the working interface of an associated interface pair.
aps y-cable	Configures y-cable line card protection.
associate group	Creates or specifies an APS interface group and enters APS configuration mode.
associate interface	Associates wavepatch interfaces for APS splitter protection.
show aps trace	Shows APS and APS channel protocol activity information.

Cisco ONS 15540 ESPx Command Reference Guide

show aps trace

To display APS and APS channel protocol activity information in the system memory, use the **show aps trace** command.

show aps trace [clear | stop | resume]

Syntax Description

clear	Clears the APS activity trace table in memory.
stop	Stops the collection of APS activity information.
resume	Resumes the collection of APS activity information.

Defaults

Displays APS and APS channel protocol activity information.

Trace is active.

Command Modes

EXEC and privileged EXEC

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines

APS trace information is similar to **show aps** command output except that it is stored in processor memory. The trace buffer contains activity information for APS and for the APS channel protocol.

The trace collection status and information are not saved across system or processor card reloads. After the reload, the trace status returns to the default active state and the trace buffer in memory is cleared.

Examples

The following example shows how to clear the APS trace buffer.

```
Switch# show aps trace clear
```

The following example shows how to stop the APS trace activity information collection.

```
Switch# show aps trace stop
```

The following example shows how to resume the APS trace activity information collection.

```
Switch# show aps trace resume
```

The following example shows how to display detailed APS information for all APS groups. (See Table 1-3 for field descriptions.)

```
Switch# show aps trace
APS: Wavepatch10/0/0: searchup timer expired
APS: Wave10/0: wave state WAVE_DOWN
APS: wp event SEARCHUP_EXP: wv state WAVE_DOWN
APS: switch optk swpos to 1
APS: restart searchup timer: check after 32 sec
ACP: Wavepatch10/0/0: service request timer
ACP: Wavepatch10/0/0: xmit request failed: protection oscp idb missing
ACP: Transparent10/0/0: service request timer
ACP: Transparent10/0/0: xmit request failed: neither y-cable nor splitter
ACP: Wavepatch10/0/0: service request timer
ACP: Wavepatch10/0/0: xmit request failed: protection oscp idb missing
ACP: Transparent10/0/0: service request timer
ACP: Transparent10/0/0: xmit request failed: neither y-cable nor splitter
APS: Wavepatch10/0/0: searchup timer expired
APS: Wave10/0: wave state WAVE_DOWN
APS: wp event SEARCHUP_EXP: wv state WAVE_DOWN
APS: switch optk swpos to 0
APS: restart searchup timer: check after 32 sec
ACP: Transparent10/0/0: service request timer
ACP: Transparent10/0/0: xmit request failed: neither y-cable nor splitter
```

Table 1-3   show aps trace Field Descriptions

Field	Description
APS:	Specifies APS activity.
ACP:	Specifies APS channel protocol activity.

Related Commands

Command	Description
associate interface	Associates two interfaces for APS protection.
debug aps	Enables debugging of APS and APS channel protocol.
show aps	Shows APS configuration and status information.

Debug Commands

Use the following commands to debug the Cisco ONS 15540 ESPx. For information on other debug commands refer to the *Cisco IOS Debug Command Reference* document.

debug aps

To debug APS operation, use the **debug aps** command. To disable APS debugging, use the **no** form of this command.

debug aps

no debug aps

Syntax Description   This command has no other arguments or keywords.

Defaults   Disabled

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   To turn off all debugging, use the **undebug all** command.

Examples   The following example shows how to enable debugging of APS operations.

```
Switch# debug aps
```

Related Commands

Command	Description
associate group	Creates or specifies an APS interface group and enters APS configuration mode.
associate interface	Associates wavepatch interfaces for APS splitter protection.
undebug all	Disables all debugging.

debug cdl defect-indication

To enable debugging for the in-band message channel, use the **debug cdl defect-indication** command. To disable debugging for online diagnostics, use the **no** form of this command.

> **debug cdl defect-indication** {**error** | **events** | **periodic**}

> **no debug cdl defect-indication** {**error** | **events** | **periodic**}

Syntax Description

error	Enables debugging for in-band message channel error conditions.
events	Enables debugging for in-band message channel internal software event conditions.
periodic	Enables debugging for in-band message channel periodic events.

Defaults   Disabled

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines Use this command to enable debugging for the message channel.

To turn off all debugging, use th**e no debug cdl defect-indication co**mmand.

Examples   The following example shows how to enable debugging of background tests for the message channel.

```
Switch# debug cdl defect-indication
```

Related Commands	Command	Description
	diag online	Enables online diagnostics for the system.
	diag online slot	Enables online diagnostics for a specified slot number.
	show cdl defect-indication	Displays cdl defect-indication information.
	undebug all	Disables all debugging.

debug cpu

To debug IPC (interprocess communication) initialization and switchover events, use the **debug cpu** command. To disable debugging IPC initialization and switchover events, use the **no** form of this command.

debug cpu {**ehsa** | **intf-sync** | **ipc** | **redundancy** | **sub-ipc**}

no debug cpu {**ehsa** | **ipc** | **redundancy** | **sub-ipc**}

ehsa	Enables debugging for processor EHSA (enhanced high system availability) services such as hostname, config register, and calendar synchronizing to the standby processor card.
intf-sync	Enables debuggin for interface sync RF events
ipc	Enables debugging for processor IPC (interprocessor communications) initialization and switchover events.
pwd-sync	Enables debugging for password sync RF events
redundancy	Enables debugging for processor card redundancy initialization and operation.
snap	Enables debugging for low level SNAP communication.
sub-ipc	Enables debugging for the IPC channel layer below the IPC level.

Syntax Description (label at left)

Defaults   Disabled

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	Modification
12.2(18)SV	This command was integrated in this release.
S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to enable debugging of IPC initialization and switchover events. To debug redundancy software operations, use the **debug redundancy** command.

To turn off all debugging, use the **undebug all** command.

Examples   The following example shows how to enable redundancy state debugging.

```
Switch# debug cpu redundancy
```

Related Commands

Command	Description
debug redundancy	Enables debugging of redundancy software operation.
undebug all	Disables all debugging.

debug diag online

To enable debugging for online diagnostics, use the **debug diag online** command. To disable debugging for online diagnostics, use the **no** form of this command.

debug diag online [**online-insertion-removal** | **background** | **redundancy**]

no debug diag online [**online-insertion-removal** | **background** | **redundancy**]

Syntax Description

online-insertion-removal	Enables debugging of OIR (online insertion and removal) tests for online diagnostics.
background	Enables debugging of background tests for online diagnostics.
redundancy	Enables debugging of redundancy tests for online diagnostics.

Defaults   Disabled

Command Modes   Privileged EXEC

Command History This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines Use this command to enable debugging for online diagnostics.

To turn off all debugging, use the **undebug all** command.

Examples   The following example shows how to enable debugging of background tests for online diagnostics.

```
Switch# debug diag online background
```

Related Commands

Cisco ONS 15540 ESPx Command Reference Guide

Command	Description
show diag online	Enables online diagnostics for the system.
diag online slot	Enables online diagnostics for a specified slot number.
undebug all	Disables all debugging.

debug driver control ethernet

To enable backplane Ethernet driver debugging, use the **debug driver control ethernet** command. To disable backplane ethernet driver debugging operations, use the **no** form of this command.

> **debug driver control ethernet** {**errors** | **events** | **packets**}

> **no debug driver control ethernet** {**errors** | **events** | **packets**}

Syntax Description

errors	Enables debugging for SRC driver error conditions.
events	Enables debugging for internal software error conditions.
packets	Enables debugging of the backplane Ethernet drive packets.

Defaults   Disabled

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to activate backplane Ethernet driver debugging.

Examples   The following example shows how to activate backplane Ethernet driver error debugging.

```
Switch# debug driver control ethernet errors
```

Related Commands

Command	Description
debug aps	Enables debugging of APS and APS Channel Protocol activity.
debug cpu	Enables debugging of IPC initialization and switchover events.

Cisco ONS 15540 ESPx Command Reference Guide

Command	Description
debug diag online	Enables debugging of the online diagnostics.
debug ports	Enables debugging of optical port activity.
debug redundancy	Enables debugging of redundancy software operation.

debug driver nvram

To enable Cisco ONS 15540 ESPx NVRAM file system debugging, use the **debug driver nvram** command. To disable Cisco ONS 15540 ESPx NVRAM file system debugging operations, use the **no** form of this command.

> **debug driver nvram** {**errors** | **events**}

> **no debug driver nvram** {**errors** | **events**}

Syntax Description

errors	Enables debugging for NVRAM driver error conditions.
events	Enables debugging for internal software events.

Defaults   Disabled

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to enable NVRAM file system platform specific debugging.

Examples   The following example shows how to activate NVRAM file system platform specific debugging.

```
Switch# debug driver nvram errors
```

Related Commands

Command	Description
debug aps	Enables debugging of APS and APS Channel Protocol activity.
debug cpu	Enables debugging of IPC initialization and switchover events.

Cisco ONS 15540 ESPx Command Reference Guide

Command	Description
debug diag online	Enables debugging of the online diagnostics.
debug ports	Enables debugging of optical port activity.
debug redundancy	Enables debugging of redundancy software operation.

debug driver psm

To enable the PSM driver debugging, use the **debug driver psm** command. To disable PSM driver debugging, use the **no** form of this command.

debug driver psm {**errors** | **events**}

no debug driver psm {**errors** | **events**}

Syntax Description

errors	Enables debugging for PSM driver error conditions.
events	Enables debugging for internal software events.

Defaults   Disabled

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to activate the PSM driver debugging.

Examples   The following example shows how to activate the PSM driver error debugging.

```
Switch# debug driver psm errors
```

Related Commands

Command	Description
debug aps	Enables debugging of APS and APS Channel Protocol activity.
debug ports	Enables debugging of optical port activity.

debug driver src

To enable SRC driver debugging, use the **debug driver src** command. To disable SRC driver debugging operations, use the **no** form of this command.

> **debug driver src** {**errors** | **events** | **poll-errors** | **portfail** | **defect-indication** {**errors** | **events** | **periodic**}}

> **no debug driver src** {**error** | **events** | **poll-errors** | **portfail** | **defect-indication** {**errors** | **events** | **periodic**}}

Syntax Description

errors	Enables debugging for NVRAM driver error conditions.
events	Enables debugging for SRC driver events.
poll-errors	Enables debugging for internal software error conditions.
portfail	Enables debugging for port failures.
defect-indication {errors	events	periodic}	Enables debugging for defect indications.

Defaults   Disabled

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to activate SRC driver debugging.

Examples   The following example shows how to activate SRC driver debugging.

```
Switch# debug driver src
```

Related Commands	Command	Description
	debug aps	Enables debugging of APS and APS Channel Protocol activity.
	debug cpu	Enables debugging of IPC initialization and switchover events.
	debug diag online	Enables debugging of the online diagnostics.
	debug ports	Enables debugging of optical port activity.
	debug redundancy	Enables debugging of redundancy software operation.

debug driver transparent events

To enable transparent driver debugging, use the **debug driver transparent events** command. To disable transparent driver debugging, use the **no** form of this command.

debug driver transparent events

no debug driver transparent events

Syntax Description   This command has no other arguments or keywords.

Defaults   Disabled

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to activate transparent driver debugging.

Examples   The following example shows how to enable the **debug driver transparent** command.

```
switch# debug driver transparent events
```

Related Commands

Command	Description
debug aps	Enables debugging of APS and APS Channel Protocol activity.
debug ports	Enables debugging of optical port activity.

debug ip ssh client

To debug , use the command. To disable debugging for , use the **no** form of this command.

debug ip ssh client{ | } []

no debug ip ssh client{ | } []

Syntax Description

Defaults

Disabled

Command Modes

Privileged EXEC

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to enable debugging for OSCP activity.

To disable all debugging, use the **undebug all** command.

⚠️ **Caution** This command can generate a significant amount of output and may interfere with other activity on the system once the command is invoked.

Examples

The following example shows how to enable debugging for OSCP events.

```
Switch# debug oscp events
01:53:59:Control interface Wave1 is going up
```

```
01:54:00:OSCP:Adding neighbor on wave Wave1
```

The following example shows how to display information contained in the OSCP Hello packets.

```
Switch# debug oscp hello-packet wave 0
01:53:08:OSCP:Hello at Wave1 Tx, state 2way
01:53:08:  NodeId:0202.0304.0506  Port:10000
01:53:08:  Remote:NodeId:0202.0304.0506  Port:10000
01:53:08:OSCP:Hello at Wave1 Rx, state 2way
01:53:08:  NodeId:0202.0304.0506  Port:10000
01:53:08:  Remote:NodeId:0202.0304.0506  Port:10000
01:53:08:OSCP:Hello event 2wayd
```

Related Commands

Command	Description
show oscp info	Displays OSCP configuration information.
show oscp neighbor	Displays OSCP neighbor information.
show oscp statistics	Displays OSCP activity statistics.
show oscp traffic	Displays OSCP message traffic information.
undebug all	Disables all debugging.

debug oscp

To debug OSCP operations, use the **debug oscp** command. To disable debugging for OSCP operations, use the **no** form of this command.

> **debug oscp** {**events** | **hello-packet** | **transport**} [**wave** *slot*]

> **no debug oscp** {**events** | **hello-packet** | **transport**} [**wave** *slot*]

Syntax Description

events	Enables debugging for OSCP events.
hello-packet	Enables printing of the information contained in the OSCP Hello packets.
transport	Enables debugging for OSCP transport services.
wave *slot*	Specifies the OSC interface on which to enable debugging. (Optional)

Defaults   Disabled

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to enable debugging for OSCP activity.

To disable all debugging, use the **undebug all** command.

⚠
Caution   This command can generate a significant amount of output and may interfere with other activity on the system once the command is invoked.

Examples   The following example shows how to enable debugging for OSCP events.

```
Switch# debug oscp events
```

Cisco ONS 15540 ESPx Command Reference Guide

```
01:53:59:Control interface Wave1 is going up
01:54:00:OSCP:Adding neighbor on wave Wave1
```

The following example shows how to display information contained in the OSCP Hello packets.

```
Switch# debug oscp hello-packet wave 0
01:53:08:OSCP:Hello at Wave1 Tx, state 2way
01:53:08:  NodeId:0202.0304.0506  Port:10000
01:53:08:  Remote:NodeId:0202.0304.0506  Port:10000
01:53:08:OSCP:Hello at Wave1 Rx, state 2way
01:53:08:  NodeId:0202.0304.0506  Port:10000
01:53:08:  Remote:NodeId:0202.0304.0506  Port:10000
01:53:08:OSCP:Hello event 2wayd
```

Related Commands	Command	Description
	show oscp info	Displays OSCP configuration information.
	show oscp neighbor	Displays OSCP neighbor information.
	show oscp statistics	Displays OSCP activity statistics.
	show oscp traffic	Displays OSCP message traffic information.
	undebug all	Disables all debugging.

debug ports

To debug port operations, use the **debug ports** command. To disable debugging for port operations, use the **no** form of this command.

> **debug ports** {**connect** | **errors** [*type slot*[*/subcard*[*/port*]]] | **events** [*type slot*[*/subcard*[*/port*]]] | **patch**}

> **no debug ports** {**connect** | **errors** [*type slot*[*/subcard*[*/port*]]] | **events** [*type slot*[*/subcard*[*/port*]]] | **patch**}

Syntax Description

connect	Enables debugging for cross connections.
errors	Enables debugging for internal software error conditions.
type slot[*/subcard*[*/port*]]	Specifies an interface on which debugging is enabled. Valid *type* values are **filter**, **tengigethernetphy**, **thru**, **transparent**, **wave**, **waveethernetphy**, **wavepatch**, **wdm**, and **wdmsplit**. (Optional)
events	Enables debugging for internal software event conditions.
patch	Enables debugging for patch connections.

Defaults   Disabled

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to debug common software errors and events, patch connection activity, and cross connection activity. If the interface option is not specified, debugging is enabled for all interfaces.

To disable all debugging, use the **undebug all** command.

Examples   The following example shows how to enable error debugging for transparent interface 2/0/0.

```
Switch# debug ports errors transparent 2/0/0
```

Related Commands

Command	Description
clock rate	Configures a clock rate on a transparent interface.
clear performance history	Configures the encapsulation of the client signal on the transparent interface.
monitor enable	Enables signal monitoring for certain protocol encapsulations.
patch	Configures patch connections for a shelf.
show connect	Displays optical connection information.
show interfaces	Displays interface information.
patch	Displays optical patch connection configuration.
undebug all	Disables all debugging.

debug redundancy

To debug redundancy operations, use the **debug redundancy** command. To disable debugging for redundancy operations, use the **no** form of this command.

> **debug redundancy** {**ehsa** | **errors** | **fsm** | **kpa** | **msg** | **progression** | **status** | **timer**}

> **no debug redundancy** {**ehsa** | **errors** | **fsm** | **kpa** | **msg** | **progression** | **status** | **timer**}

Syntax Description

ehsa	Enables debugging for early software initialization suspend points associated with EHSA (enhanced high system availability).
errors	Enables debugging for redundancy internal software error conditions.
fsm	Enables debugging for redundancy finite state machine transition events.
kpa	Enables debugging for redundancy keepalive messaging events.
msg	Enables debugging for general redundancy messaging software.
progression	Enables debugging for redundancy internal state progression software.
status	Enables debugging for redundancy internal status notification software.
timer	Enables debugging for redundancy internal timers.

Defaults   Disabled

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to debug redundancy software operations. Use the **debug cpu** command to debug processor card redundancy.

To disable all debugging, use the **undebug all** command.

Cisco ONS 15540 ESPx Command Reference Guide

⚠

Caution   This command can generate a significant amount of output and may interfere with other activity on the system once the command is invoked.

Examples   The following example shows how to debug finite state machine transition events.

```
Switch# debug redundancy fsm
```

Related Commands

Command	Description
debug cpu	Enables debugging of processor card redundancy.
show redundancy summary	Displays processor card redundancy status and configuration information.
undebug all	Disables all debugging.

undebug all

To disable all debugging, use the **undebug all** command.

undebug all

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to turn off all debugging.

Examples   The following example shows how to turn off all debugging.

```
Switch# undebug all
```

Related Commands

Command	Description
debug aps	Enables debugging of APS and APS Channel Protocol activity.
debug cpu	Enables debugging of IPC initialization and switchover events.
debug diag online	Enables debugging of the online diagnostics.
debug oscp	Enables debugging of OSCP activity.
debug ports	Enables debugging of optical port activity.
debug redundancy	Enables debugging of redundancy software operation.

Cisco ONS 15540 ESPx Command Reference Guide

undebug all

3

Interface Configuration Commands

Use the following commands to configure and monitor the interfaces on the Cisco ONS 15540 ESPx.

clock rate

To configure the signal clock rate without an associated protocol on a transparent interface, use the **clock rate** command. To disable the clock rate, use the **no** form of this command.

clock rate *value*

no clock rate

Syntax Description

value	Specifies the signal rate. The range is 16000 to 2500000 kHz.

Defaults   Disabled

Command Modes   Interface configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   You can configure the signal clock rate with either the **cdl defect-indication force hop-endpoint** command or the **clock rate** command, but not both. Protocol monitoring cannot be enabled on the interface when the **clock rate** command is configured because no protocol is specified.

Table 3-1 lists the clock rates for well-known protocols supported by the 2.5-Gbps transponder module.

Table 3-1   Supported Clock Rates for Well-Known Protocols

Well-Known Protocol	Clock Rate (in kbps)
DS3	44,736
DV1[1] in ADI[2] mode	270,000
E3	34,368
ESCON	200,000
Fibre Channel (1 Gbps)	1,062,500

Table 3-1   Supported Clock Rates for Well-Known Protocols (continued)

Well-Known Protocol	Clock Rate (in kbps)
Fibre Channel (2 Gbps)	2,125,000
FICON (1 Gbps)	1,062,500
FICON (2 Gbps)	2,125,000
Gigabit Ethernet	1,250,000
ISC compatibility mode (ISC-1)	1,062,500
ISC peer mode (ISC-3)	2,125,000
SONET OC-1	51,840
SONET OC-3/SDH STM-1	155,520
SONET OC-12/SDH STM-4	622,080
SONET OC-24	933,120
SONET OC-48/SDH STM-16	2,488,320

1. DV = digital video

2. ADI = Asynchronous Digital Interface

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

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

- 851,000 kbps to 999,999 kbps

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

For clock rate values outside of these unsupported ranges and not listed in Table 3-1, contact your SE (systems engineer) at Cisco Systems.

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

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

Examples   The following example shows how to configure the signal clock rate on an interface.

```
Switch# configure terminal
Switch(config)# interface transparent 10/0/0
```

Chapter 3   Interface Configuration Commands

■   clock rate

```
Switch(config-if)# clock rate 125000
```

Related Commands	Command	Description
	clear performance history	Specifies the protocol encapsulation for a transparent interface.
	show interfaces	Displays interface information.

cdl defect-indication force hop-endpoint

To configure an interface as an end-of-hop, use the **cdl defect-indication force hop-endpoint** command. To disable end-of-hop configuration on an interface, use the **no** form of this command.

cdl defect-indication force hop-endpoint

no cdl defect-indication force hop-endpoint

Syntax Description   This command has no other arguments or keywords.

Defaults   Disabled

Command Modes   Interface configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV2	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to configure the interface as a hop endpoint for in-band message channel defect indications.

Examples   The following example shows how to enable hop endpoint on an interface.

```
Switch# configure terminal
Switch(config)# interface waveethernetphy 8/0
Switch(config-if)# cdl defect-indication force hop-endpoint
```

Cisco ONS 15540 ESPx Command Reference Guide

Related Commands	Command	Description
	debug cdl defect-indication	Initiates debugging of defect indication on in-band message channel capable interfaces.
	show cdl defect-indication	Displays defect indication information on in-band message channel capable interfaces.
	show interfaces	Displays interface information.

cdl enable

To enable in-band message channel functionality on an interface, use the **cdl enable** command. To disable in-band message channel functionality, use the **no** form of this command.

cdl enable

no cdl enable

Syntax Description   *This command has no other arguments or keywords.*

Defaults   Disabled

Command Modes   Interface configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV2	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   This command is used to enable and disable the in-band message channel on tengigethernetphy interfaces when connected to a Cisco ONS 15530 or any other system that supports the in-band message channel. When the in-band message channel is enabled on a tengigethernetphy interface, ethernetdcc *slot/subcard/1* becomes available for configuration.

Examples   The following example shows how to enable in-band message channel on an interface.

```
Switch# configure terminal
Switch(config)# interface tengigethernetphy 10/0
Switch(config-if)# cdl enable
```

Related Commands

Command	Description
cdl defect-indication force hop-endpoint	Configures an interface as an end-of-hop.
clear performance history	Specifies the in-band message channel flow identifier value.
debug cdl defect-indication	Initiates debugging of the defect indication on in-band message channel capable interfaces.
show cdl defect-indication	Displays defect indication information on in-band message channel capable interfaces.
show interfaces	Displays interface information.

clear performance history

To clear and reset the performance history counters, use the **clear performance history** command.

clear performance history [*interface*]

Syntax Description

interface	Specifies the interface on which the command is to be executed.

Defaults

Clears all the performance history counters (the current counter, all 15-minute history counters, and the 24-hour counter) for all Cisco ONS 15540 ESPx interfaces.

Command Modes

EXEC and privileged EXEC.

Command History

This table includes the following release-specific history entries:

SV-Release	Modification
12.2(29)SV	This command was introduced.

Usage Guidelines

Use this command to clear and reset the performance history counters.

Examples

The following example shows how to clear the performance history counters for a transparent interface.

```
Switch# clear performance history transparent 8/0/0
Reset performance history on interface?[confirm]y
Switch#
```

Related Commands

Command	Description
show performance	Displays the performance history counters for the specified interface.
clear counters	Clears all the interface counters.
auto-sync counters interface	Enables the automatic synchronization of the performance history counters and interface counters.

encapsulation

To configure the protocol encapsulation for the client signal on a transparent interface, use the **encapsulation** command. To disable the encapsulation for the client signal, use the **no** form of this command.

> **encapsulation** {**fastethernet** |
>   **fddi** |
>   **gigabitethernet** |
>   **escon** |
>   **sysplex** {**clo** | **etr** | **isc** {**compatibility** | **peer** [**1g** | **2g**]}}
>   **ficon** {**1g** | **2g**} |
>   **sonet** {**oc3** | **oc12** | **oc48**} |
>   **sdh** {**stm-1** | **stm-4**| **stm-16**} |
>   **fibrechannel** {**1g** | **2g**} [**ofc** {**enable** | **disable**}]}}

> **no encapsulation**

Syntax Description

fastethernet	Specifies Fast Ethernet encapsulation. The OFC (open fiber control) safety protocol is disabled.
fddi	Specifies FDDI encapsulation. OFC is disabled.
gigabitethernet	Specifies Gigabit Ethernet encapsulation. OFC is disabled.
escon	Specifies ESCON encapsulation. OFC is disabled.
sysplex	Specifies Sysplex encapsulation. **Note** This encapsulation is only supported on multimode transponder modules.
clo	Specifies CLO (control link oscillator) timing. OFC is disabled. Forward laser control is enabled on both the transparent and wave interfaces.
etr	Specifies ETR (external timer reference) timing. OFC is disabled.
isc	Specifies ISC (InterSystem Channel) encapsulation.
compatibility	Specifies ISC compatibility mode (ISC1) with rate of 1.0625 Gbps. OFC is enabled.
peer [**1g**	**2g**]	Specifies ISC peer mode (ISC3) and rate. OFC is disabled. The default rate is 2.1 Gbps.
ficon {**1g**	**2g**}	Specifies FICON encapsulation and rate. OFC is disabled.
sonet {**oc3**	**oc12**	**oc48**}	Specifies SONET encapsulation and rate. OFC is disabled.
sdh {**stm-1**	**stm-4**	**stm-16**}	Specifies SDH encapsulation and rate. OFC is disabled.
fibrechannel rate {**1g**	**2g**}	Specifies Fibre Channel encapsulation and rate.
ofc {**enable**	**disable**}	Enables or disables OFC. The default OFC state is disabled. (Optional)

Defaults   Encapsulation is disabled.

The default rate for ISC peer mode is **2g**.

See the "Syntax Description" section for the default OFC state.

Command Modes   Interface configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
12.1(12c)EV1	Added support for 2-Gbps FC and FICON.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
12.2(23)SV	Added support for 1-Gbps ISC links peer mode.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.
12.2(25)S	Added support for 1-Gbps ISC links peer mode.

Usage Guidelines   Use this command to provide clocking for the client signal for specific protocols. The protocol encapsulation must be configured for the transparent interface to allow signal monitoring to be enabled with the **monitor enable** command. 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
- ISC links peer mode (1 Gbps and 2 Gbps)
- 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
- FDDI

■ **encapsulation**

- Sysplex CLO (control link oscillator)

- Sysplex ETR (external timer reference)

To specify the signal clock rate without specifying a protocol, use the **clock rate** command.

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

Note Encapsulation cannot be changed without first disabling monitoring using the **no monitor enable** command.

Removing the encapsulation on a transparent interface with the **no encapsulation** command does not turn off the laser. To turn off the transmit laser to the client equipment, use the **show performance** command.

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

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

Examples   The following example shows how to configure SONET encapsulation at a rate of OC-3 on a transparent interface.

```
Switch# configure terminal
Switch(config)# interface transparent 2/0/0
Switch(config-if)# encapsulation sonet oc3
```

Related Commands

Command	Description
clock rate	Configures a clock rate on a transparent interface.
monitor enable	Enables signal monitoring for certain protocol encapsulations.
show interfaces	Displays interface information.
show performance	Disables an interface.

laser control forward enable

To enable forward laser control, which automatically shuts down transponder lasers when a Loss of Light failure occurs, use the **laser control forward enable** command. To disable this feature, use the **no** form of this command.

> **laser control forward enable**
>
> **no laser control forward**

Syntax Description   This command has no other arguments or keywords.

Defaults   Disabled

Command Modes   Interface configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to enable forward laser control on both the client side and trunk side interfaces of a transponder module and on the OSC wave interfaces. If configured on a transparent interface, the client side laser of the transponder shuts down when the trunk side receiver detects a Loss of Light. If configured on the wave interface, the trunk side laser of the transponder shuts down when client side receiver detects a Loss of Light.

> **Note**   To function correctly, configure forward laser control on both the client side and trunk side interfaces on a transponder module. CSCdu42900 For y-cable protection, configure forward laser control on both the client side and trunk side interfaces on both transponder modules.

Automatically shutting down the laser prevents the transmission of unreliable data. However, when the laser is shut down, fault isolation is more difficult.

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

⚠

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 enable forward laser control on a transparent interface.

```
Switch# configure terminal
Switch(config)# interface transparent 3/2/0
Switch(config-if)# laser control forward enable
```

The following example shows how to enable forward laser control on a wave interface.

```
Switch# configure terminal
Switch(config)# interface wave 2/0
Switch(config-if)# laser control forward enable
```

Related Commands

Command	Description
show interfaces	Displays interface information.

laser control safety enable

To enable laser safety control on a wave interface, use the **laser control safety enable** command. To disable laser safety control, use the **no** form of this command.

laser control safety enable

no laser control safety

Syntax Description   This command has no other arguments or keywords.

Defaults   Disabled

Command Modes   Interface configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to automatically shut down the lasers transmitting to the trunk fiber when a Loss of Light failure occurs, such as a trunk fiber cut. Enable laser safety control on all wave interfaces in the shelf, including the OSC wave interface.

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 durations timers compliant with the ALS (automatic laser shutdown) standard (ITU-T G.664).

Note   This command is not supported on waveethernetphy interfaces.

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

⚠

Caution   Use this command only with line card protected configurations or unprotected configurations.

Examples   The following example shows how to enable laser safety control on a wave interface.

```
Switch# configure terminal
Switch(config)# interface wave 2/0
Switch(config-if)# laser control safety enable
```

Related Commands

Command	Description
show interfaces	Displays interface information.

laser frequency

To select the desired channel frequency on a transparent transponder, use the **laser frequency** command. To revert to the default value, use the **no** form of the command.

laser frequency *value*

no laser frequency

Syntax Description

value	Laser frequency in GHz.

Defaults   The lower frequency for the interface is the default.

Command Modes   Interface configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   The transparent transponders can be tuned to support one of two channel frequencies. The **laser frequency** command allows the user to change the laser tuning from the default lower frequency to the higher frequency, and back.

The change from one frequency to another takes about 10 seconds. Do not expect traffic to transit the system until the frequency selection completes. Also, successive **laser frequency** commands are ignored until after the new channel frequency stabilizes.

Examples   The following example shows how to select the channel frequency on a transponder wave interface.

```
Switch(config)# interface wave 3/0
Switch(config-if)# laser frequency 192300
```

Related Commands	Command	Description
	show connect	Displays optical connection information.
	show interfaces	Displays interface information.

laser shutdown

To turn off the laser on an interface supporting the in-band message channel, use the **laser shutdown** command. To turn the laser on, use the **no** form of this command.

laser shutdown

no laser shutdown

Syntax Description   This command has no other arguments or keywords.

Defaults   The laser is on.

Command Modes   Interface configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV2	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to explicitly shut down the laser. The interface **shutdown** command disables data traffic; however, the control traffic carried over in-band message channel continues to flow. Use this command to turn off the laser and stop all traffic.

Note   The interface **shutdown** command must precede the **laser shutdown** command. To bring the interface administratively up, the **no laser shutdown** must precede the **no shutdown** command.

Note   If you turn off the laser on an interface and save the configuration to the startup configuration, the interface comes up with the laser turned off when the system boots.

Note   A 10-Gbps laser on a waveethernetphy interface must warm up for 2 minutes before carrying traffic.

Examples   The following example shows how to turn off the laser on a waveethernetphy interface.

```
Switch(config)# interface waveethernetphy 4/0
Switch(config-if)# laser shutdown
```

Related Commands

Command	Description
show interfaces	Displays interface information.

loopback

To configure a signal loopback on transponder module interfaces, use the **loopback** command. To disable interface loopback, use the **no** form of this command.

loopback

no loopback

Syntax Description   This command has no other arguments or keywords.

Defaults   Disabled

Command Modes   Interface configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to configure internal loopbacks on transponder module interfaces. For any given transponder module, you can configure an internal loopback on either the client side interface or the trunk side interface, but not both simultaneously.

An internal loopback differs from an external loopback where you simply run a cable from the output of a given interface to its input. Using the **loopback** command, you can set loopbacks *without* the need to change the cabling. This is useful for remote testing, configuration, and troubleshooting.

Note   If you enable loopback on an interface and save the configuration to NVRAM, the interface comes up with loopback enabled when the system boots.

Examples   The following example shows how to enable loopback on a transparent interface.

```
Switch# configure terminal
```

Cisco ONS 15540 ESPx Command Reference Guide

```
Switch(config)# interface transparent 2/0/0
Switch(config-if)# loopback
```

The following example shows how to enable loopback on a wave interface.

```
Switch# configure terminal
Switch(config)# interface wave 10/0
Switch(config-if)# loopback
```

Related Commands	Command	Description
	show interfaces	Displays interface information.

monitor enable

To monitor signal quality and protocol error statistics in the transponder module, use the **monitor enable** command. To disable monitoring, use the **no** form of this command.

monitor enable

no monitor

Syntax Description   This command has no other arguments or keywords.

Defaults   Disabled

Command Modes   Interface configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release and added monitoring support for 2-Gbps Fibre Channel and FICON.
12.2(22)SV	Added monitoring support for 2-Gbps ISC links peer mode.
12.2(23)SV	Added monitoring support for 1-Gbps ISC links peer mode.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.
12.2(25)S	Added monitoring support for 1-Gbps ISC links peer mode.

Usage Guidelines   Use this command to collect error statistics on signal quality in the transponder module. The following protocols can be monitored:

- 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
- ISC links peer mode (1 Gbps and 2 Gbps)

- 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

When monitoring is enabled on the transparent interface, it is automatically enabled on the corresponding wave interface.

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

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

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

- Loss of Light
- Loss of Lock (when the clock cannot be recovered from the received data stream)
- Severely Errored Frame
- Loss of Frame

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

The source of the acronym definitions is the Telcordia SONET standard spec, GR-253-CORE, Issue 3, September 2000, page 6-110,

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

For ISC traffic, the system monitors the following conditions:

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

Note Before monitoring can be enabled, you must configure protocol encapsulation for the interface using the **cdl defect-indication force hop-endpoint** command.

Monitoring signal error statistics is useful for isolating system and network faults.

Examples The following example shows how to monitor error counters on a transparent interface.

```
Switch# configure terminal
Switch(config)# interface transparent 2/0/0
Switch(config-if)# monitor enable
```

Related Commands

Command	Description
clear performance history	Configures the encapsulation of the client signal on the transparent interface.
show interfaces	Displays interface information.

optical threshold power receive

To set the receive optical threshold power for alarms on wdm, thru, and wavepatch interfaces, use the **optical threshold power receive** command.To revert to the default values, use the **no** form of the command.

> **optical threshold power receive {low | high} {alarm | warning}** *value* **[severity {critical | major | minor | not alarmed | not reported}]**

> **no optical threshold power receive**

Syntax Description	before-amplification	Indicates that the threshold is on parameter value as seen before passing through optical amplifier. This keyword is not present when there is no optical amplifier at this interface.
	after-amplification	Indicates that the threshold is on parameter value as seen after passing through optical amplifier. This keyword is not present when there is no optical amplifier at this interface.
	low	Specifies a low threshold value.
	high	Specifies a high threshold value.
	alarm	Indicates that an alarm is raised when the threshold is exceeded.
	warning	Indicates that a warning is reported when the threshold is exceeded. The severity of a warning threshold must be less than the severity of the corresponding alarm threshold.
	value	Sets the threshold value in tenths of a dBm. The range is –80 to –280 for 2.5-Gbps transponder modules and –80 to –220 for 10-GE transponder modules.
	severity	Specifies the severity for the threshold.
	critical	Indicates the threshold level for service-affecting conditions that require immediate corrective action.
	major	Indicates the threshold level for hardware or software conditions that cause serious service disruption, or malfunctioning or failure of important hardware. These problems require the immediate attention and response of a technician to restore or maintain system capability. The urgency is less than in critical situations because of a lesser immediate or impending effect on service or system performance. This is the default value for alarms.
	minor	Indicates the threshold level for problems that do not have a serious effect on service, or for problems in hardware that do not affect the essential operation of the system.
	not alarmed	Indicates the threshold level for negligible discrepancies, and that do not cause alarm notifications to be generated. The information for these events is retrievable from the network element. This is the default value for warnings.
	not reported	Indicates the threshold level for negligible discrepancies, and that do not cause notifications to be generated. The information for these events is retrievable from the network element.

Defaults

Alarm severity: **major**

Warning severity: **not alarmed**

Interface Type	Low Alarm	Low Warning	High Warning	High Alarm
Wavepatch on a 2.5-Gbps transponder module	–28 dBm	–24 dBm	–10 dBm	–8 dBm
Wavepatch on a 10-GE transponder module	–22 dBm	–20 dBm	–10 dBm	–8 dBm
wdm	–30 dBm	–	18 dBm	–
thru	–30 dBm	–	18 dBm	–

Command Modes

Interface configuration

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
12.1(12c)EV2	The default values for the 10-GE transponder module high warning and high alarm were changed.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines

The default value for high alarm threshold corresponds to the receiver saturation level for the transponder module.

The default value for low alarm threshold corresponds to the Loss of Light condition. Exceeding the low alarm threshold on the active wavepatch interface causes a protection switchover to the standby wavepatch interface, provided that the standby interface is up and operating normally prior to the protection switchover.

The default values cover most network configurations. However, when optical amplifiers are used in the network in the receive direction as preamplifiers, the low alarm threshold value should be reconfigured, since the amplified noise level might be higher than the sensitivity of the receiver and the protection switchover might not be triggered. In such cases, we recommend setting the low alarm threshold to 10 dB below the power level measured at the interface when a signal exists or to –28 dB, whichever value is higher.

■   **optical threshold power receive**

> **Note** For this command to function correctly, the functional image version must be 1.A0 (or later) for multimode 2.5-Gbps transponder modules and 1.A1 (or later) for single-mode 2.5-Gbps transponder modules. Use the **show hardware** detail command to verify the functional image version.

Examples   The following example shows how to set the optical power low alarm threshold.

```
Switch(config)# interface wavepatch 8/0/0
Switch(config-if)# optical threshold power receive low alarm -210
```

Related Commands

Command	Description
show interfaces	Displays interface information.

patch

To configure the patch connections within a shelf, use the **patch** command. To remove the patch connection configuration, use the **no** form of this command.

> **patch** *interface1 [***transmit** / **receive***] interface2*

> **no patch** *interface1 [***transmit** / **receive***] interface2*

Syntax Description

interface1	Specifies the first patched interface. See the "Usage Guidelines" section for valid interface types.
transmit	Indicates that *interface1* is patched to *interface2* in the transmit direction.
receive	Indicates that *interface1* is patched to *interface2* in the receive direction.
interface2	Specifies the second patched interface. See the "Usage Guidelines" section for valid interface types.

Defaults   Both directions

Command Modes   Global configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to describe the patch connections between the mux/demux modules.

Valid patch connections between modules are:

- Wdm interface to thru interface between mux/demux modules

  wdm *slot*/*subcard1* **thru** *slot*/*subcard2*

- Thru interface to wdm interface between mux/demux modules

  thru *slot*/*subcard1* **wdm** *slot*/*subcard2*

- OSC wave interface to OSC oscfilter interface

Cisco ONS 15540 ESPx Command Reference Guide

        wave *slot* **oscfilter** *slot*/*subcard*

- OSC oscfilter interface to OSC wave interface

  oscfilter *slot*/*subcard* **wave** *slot*

- Thru interface to thru interface between mux/demux modules

  thru *slot1*/*subcard1* **thru** *slot2*/*subcard2*

- Mux/demux wdm interface to PSM wdmrelay interface

  wdm *slot*/*subcard* **wdmrelay** *slot*/*subcard*/*port*

- Wavepatch interface to filter interface

  wavepatch *slot*/*subcard*/*port* **filter** *slot*/*subcard*/*port*

- Filter interface to wavepatch interface

  filter *slot*/*subcard*/*port* **wavepatch** *slot*/*subcard*/*port*

You cannot preconfigure a patch connection. The interfaces must exist on the shelf before configuring them.

The order of the interfaces in the command does not affect the patch connect configuration. For example, configuring **patch wdm 0/1 thru 0/0** is equivalent to configuring **patch thru 0/0 wdm 0/1**.

In case of an optical interface where the transmitted and received signals travel on two different strands of fiber, it is possible that each fiber is patched to a different interface. The direction keywords **receive** and **transmit** indicate whether *interface1* is patched to *interface2* in the receive direction or the transmit direction. The absence of a keyword indicates the patch connection is bidirectional.

When one interface in a patch connection is physically removed from the shelf, the patch connection configuration persists but does not appear in the **show running-config** output. A subsequent **patch** command that includes the remaining interface overwrites the previous patch connection configuration.

Note   When a patch connection between a mux/demux module and a PSM is configured, topology learning on the wdm interface is disabled.

Examples   The following example shows how to patch a connection between two mux/demux modules in the same slot.

```
Switch# configure terminal
Switch(config)# patch wdm 1/0 thru 1/1
```

Related Commands

Command	Description
debug ports	Enables debugging of optical port activity.
show optical filter	Displays the channels supported by the mux/demux modules.
show patch	Displays optical patch connection configuration.
snmp-server enable traps patch	Enables SNMP trap notifications for patch connection activity.

show cdl defect-indication

To display the defect indication information on in-band message channel capable interfaces, use the **show cdl defect-indication** command.

show cdl defect-indication [**interface** *interface* | **detail**]

Syntax Description

detail	Displays the defect indication information for in-band message channel capable interfaces.
interface *interface*	Displays the defect indication information for a specific interface.

Defaults   Displays a defect indication summary.

Command Modes   EXEC and privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV2	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   This command displays the defect indication information on in-band message channel capable interfaces.

Examples   The following example shows how to display in-band message channel defect indication information. (See Table 3-2 for field descriptions.)

```
Switch# show cdl defect-indication
CDL Defect-Indication Status Summary
Interface     Interface   DI      Defect-Indication       Defect-Indication
Name          Status      Status      Receive                 Transmit
------------  ----------  ------  ----------------------  ----------------------
WaveE3/0      up          up          None                    None
WaveE4/0      up          up          None                    None
WaveE9/0      up          up          None                    None
WaveE10/0     up          up          None                    None
```

Table 3-2   show cdl defect-indication Field Descriptions

Field	Description
Interface Name	Shows the interface identifier.
Interface Status	Shows the interface status.
DI Status	Shows the defect indication status.
Defect-Indication Receive	Shows the defect indication on the receive signal.
Defect-Indication Transmit	Shows the defect indication on the transmit signal.

The following example shows how to display the defect indication information for in-band message channel capable interfaces.

```
Switch# show cdl defect-indication detail

Interface WaveEthernetPhy3/0
Oper.  Status: up
Admin. Status: up
Configured Node Behavior: Hop Terminating
Current Node Behavior   : Hop Terminating
Defect Indication Receive :        None
Defect Indication Transmit:        None

Interface WaveEthernetPhy4/0
Oper.  Status: up
Admin. Status: up
Configured Node Behavior: Hop Terminating
Current Node Behavior   : Hop Terminating
Defect Indication Receive :        None
Defect Indication Transmit:        None
```

Related Commands

Command	Description
cdl defect-indication force hop-endpoint	Configures an interface as an end-of-hop.
cdl enable	Enables in-band message channel functionality.
clear performance history	Specifies the in-band message channel flow identifier value.
debug cdl defect-indication	Initiates debugging of defect indication on in-band message channel capable interfaces.

show cdl flow defect-indication

To display in-band message channel defect indication information on a per-flow basis, use the **show cdl flow defect-indication** command.

> **show cdl flow defect-indication** [**interface** *interface*]

Syntax Description

interface *interface*	Displays defect indication information for a specific interface.

Defaults   Shows defect indications for all flows on the system

Command Modes   EXEC and privileged EXEC

Command History   This table includes the following release-specific history entries:

- SV-Release
- S-Release

SV-Release	Modification
12.2(18)SV	This command was first introduced.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   This command is used to display the defect indication information on in-band message channel capable interfaces.

Examples   The following example shows how to display in-band message channel flow identifier information. (See Table 3-3 for field descriptions.)

```
Switch# show cdl flow defect-indication

DI = Defect Indication

Interface          DI Received            DI Transmitted
                   from CDL network       to CDL network
------------    ---------------------- ----------------------
Tengig8/0
```

Table 3-3   show cdl flow defect-indication Field Descriptions

Field	Description
Interface	Shows the interface identifier.

Table 3-3   show cdl flow defect-indication Field Descriptions (continued)

Field	Description
DI Received from CDL network	Shows the defect indications received for the flow.
DI Transmitted to CDL network	Shows the defect indications transmitted for the flow.

Related Commands

Command	Description
cdl defect-indication force hop-endpoint	Configures an interface as an end-of-hop.
cdl enable	Enables in-band message channel functionality.
debug cdl defect-indication	Initiates debugging of defect indication on in-band message channel capable interfaces.

show connect

To display the connection relationships between the interfaces in the shelf, use the **show connect** command.

show connect {**edges** | **intermediate** [**sort-channel** | **interface** *interface*]}

Syntax Description	

edges	Displays the connections between the client-side interfaces and trunk-side interfaces of the shelf.
intermediate	Displays the complete connections between the client-side interfaces and trunk-side interfaces of the shelf, including all the intermediate internal interfaces.
sort-channel	Sorts the display by channel number.
interface *interface*	Displays the intermediate connection information for a specific interface.

Defaults None

Command Modes EXEC and privileged EXEC

Command History This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines This command shows the relationships between the interfaces in the shelf. Use this command to trace a single channel from the client side interface to the trunk side mux/demux interface.

Examples The following example shows how to display edge connection information. (See Table 3-4 for field descriptions.)

```
Switch# show connect edges
client/
wave         wdm   channel
----------   ---   -----
```

```
Trans3/0/0  1/0   26
Trans3/1/0  1/0   27
Trans3/2/0  1/0   28
Trans3/3/0  1/0   29
```

Table 3-4   show connect edges Field Descriptions

Field	Description
client/wave	Shows the client side interface identifier.
wdm	Shows the wdm interface identifier.
channel	Shows the ITU wavelength number supported by this connection.

The following example shows how to display intermediate connection information. (See Table 3-5 for field descriptions.)

```
Switch# show connect intermediate
client/         wave            wave             wdm
wave            client          patch   filter   trk   channel
------------    ------------    -------  ------   ---   -------
Trans3/0/0      Wave3/0         3/0/0*   0/0/4    0/0    5
                                3/0/1
Trans3/1/0      Wave3/1         3/1/0*   0/0/5    0/0    6
                                3/1/1
Trans3/2/0      Wave3/2         3/2/0*   0/0/6    0/0    7
                                3/2/1
Trans3/3/0      Wave3/3         3/3/0*   0/0/7    0/0    8
                                3/3/1
```

Table 3-5   show connect intermediate Field Descriptions

Field	Description
client/wave	Shows the client side interface identifier.
wave client	Shows the wave interface identifier.
wave patch	Shows the wavepatch interface identifier. The interface with the asterisk (*) carries the active signal.
filter	Shows the filter interface identifier.
wdm trk	Shows the wdm interface identifier.
channel	Shows the channel number supported by this connection.

The following example shows how to display interface connection information. (See Table 3-6 for field descriptions.)

```
Switch# show connect interface transparent 2/0/0
Client     :Transparent2/0/0
 Wave      :Wave2/0
 Wavepatch :Wavepatch2/0/0 (active)   Wavepatch :Wavepatch2/1/0
 Filter    :Filter0/0/0               Filter    :Filter1/0/0
 Wdm       :Wdm0/0                     Wdm       :Wdm1/0
 Thru      :Thru0/1                    Thru      :Thru1/1
 Wdm       :Wdm0/1                     Wdm       :Wdm1/1
 Thru      :Thru0/2                    Thru      :Thru1/2
 Wdm (trnk):Wdm0/2                     Wdm       :Wdm1/2
```

Table 3-6   *show connect interface Field Descriptions*

Field	Description
Client	Shows the client side interface identifier.
Wave	Shows the wave interface identifier.
Wavepatch	Shows the wavepatch interface identifier.
Filter	Shows the filter interface identifier.
Wdm	Shows the wdm interface identifier.
Thru	Shows the thru interface identifier.
Wdm (trnk)	Shows the identifier of the wdm interface attached to the trunk fiber.

Related Commands

Command	Description
debug ports	Enables debugging of optical port activity.
show optical filter	Displays information about the channels supported by the mux/demux modules.
show optical wavelength mapping	Displays the mapping of the Cisco ONS 15540 ESPx channels to the ITU grid wavelengths and frequencies.

show controllers

To display hardware register information for an interface, use the **show controllers** command.

show controllers [*type slot*[*/subcard*[*/port*]]]

Syntax Description	type	Specifies one of the interface types listed in Table 3-7.
	slot	Specifies a chassis slot.
	subcard	Specifies a subcard position in a motherboard.
	port	Specifies a port.

Defaults   Displays controller information for all interfaces on the system.

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
12.1(10)EV2	Support for 10-GE transponder module was added.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   The **show controllers** command displays the contents of hardware registers for the interfaces. This information is useful for troubleshooting system problems.

Table 3-7 shows the interface types for the **show controller** command.

Table 3-7   Interface Types for the show controller Command

Type	Description
fastethernet 0	Shows the NME interface information.
filter *slot/subcard/port*	Shows the filter interface information.
oscfilter *slot/subcard*	Shows the OSC oscfilter interface information.
thru *slot/subcard*	Shows the thru interface information.

Table 3-7   Interface Types for the show controller Command (continued)

Type	Description
tengigethernetphy *slot/subcard*	Shows the tengigethernetphy interface information.
transparent *slot/subcard/***0**	Shows the transparent interface information.
wave *slot*[*/subcard*]	Shows the wave interface information.
waveethernetphy *slot/subcard*	Shows the waveethernetphy interface information.
wavepatch *slot/subcard/port*	Shows the wavepatch interface information.
wdm *slot/subcard*	Shows the wdm interface information.

Examples

The following example shows how to display hardware register information about a transparent interface. (See Table 3-8 for field descriptions.)

```
Switch# show controllers transparent 3/0/0
Controller info for Transparent interface Transparent3/0/0
  LRC start addr = 0x200000
  hardware port = 1
    RCI0 monitor................:enabled
    port 1 intr SRC/CPU.........:enabled
    CPU0 MSB MAC................:0x0
    CPU0 LSB MAC................:0x0
    CPU1 MSB MAC................:0x0
    CPU1 LSB MAC................:0x0
    port error register.........:0x10000
    port ctrl msg intf mask.....:0x0
    port APS port fail mask.....:0x0
  HuJr start addr = 0x240000
  Optics control and status:
    LSC indication..............:ok
    trunk laser failure alarm...:clear
    LSC indication enable.......:disabled
    trunk laser alarm enable....:disabled
    line transceiver mode.......:non pluggable
    loss of light...............:yes
    trunk laser deviation alarm.:clear
    LSC.........................:disabled
    quick shutdown (FLC)........:disabled
    wavelength select...........:n-1 [lo wlen]
  CDR control and status:
    loss of lock................:yes
    loss of lock enable.........:disabled
  SerDes control and status:
    diags loop back.............:disabled
    line loop back..............:disabled
  GE handler control and status:
    loss of sync................:no
    loss of sync enable.........:disabled
  FC/ESCON handler control and status:
    loss of sync................:no
    loss of sync enable.........:disabled
  SONET handler control and status:
    loss of frame...............:yes
    severely errored frame......:yes
    LOF enable..................:disabled
    SEF enable..................:disabled
```

Table 3-8   show controllers Field Descriptions for Transparent Interfaces

Field	Description
Optics control and status:	Shows control and status information for the optical components in the interface.
LSC indication	Shows laser safety control status (valid only on wave interfaces).
trunk laser failure alarm	Shows the status of the trunk laser alarm. The values are: • clear—no failure • indicated—failure
LSC indication enable	Indicates whether laser safety control has been enabled (valid only on wave interfaces).
trunk laser alarm enable	Shows the status of the trunk laser alarm. If enabled, the system will signal when laser failure occurs.
Loss of Light	Indicates whether there is a Loss of Light condition.
trunk laser deviation alarm	Shows the status of the wavelength deviation alarm. If enabled, the system will signal when there is a deviation in the functioning of the laser.
LSC	Indicates whether laser safety control is enabled from the CLI (valid only on wave interfaces).
quick shutdown (FLC)	Indicates whether forward laser control is enabled on the interface (valid only on wave interfaces).
wavelength select	Indicates whether a transponder module is transmitting the lower wavelength (lo wlen) or the higher wavelength (hi wlen).
CDR control and status:	Shows the CDR (clock and data recovery) control and status information.
Loss of Lock	Indicates whether there is a Loss of Lock condition.
Loss of Lock enable	Indicates whether Loss of Lock monitoring is enabled on the interface via the **monitor enable** command.
SerDes control and status:	Shows the SerDes (serializer/deserializer) information.
GE handler control and status:	Shows Gigabit Ethernet control and status information.
Loss of Sync	Indicates whether there is a Loss of Synchronization for the signal. This field is only valid if protocol encapsulation is Gigabit Ethernet, and monitoring is enabled.
Loss of Sync enable	Indicates whether Loss of Synchronization monitoring is enabled via the **monitor enable** command.
FC/ESCON handler control and status:	Shows Fibre Channel and ESCON control and status information.
Loss of Sync	Indicates whether there is a Loss of Synchronization for the signal. This field is only valid if protocol encapsulation is Fibre Channel or ESCON, and monitoring is enabled.
Loss of Sync enable	Indicates whether Loss of Synchronization monitoring is enabled via the **monitor enable** command.
SONET handler control and status:	Shows SONET control and status information.

Table 3-8   show controllers Field Descriptions for Transparent Interfaces (continued)

Field	Description
Loss of Frame	Indicates whether there is a Loss of Frame for the signal. This field is only valid if protocol encapsulation is SONET, and monitoring is enabled.
severely errored frame	Indicates whether there is a severely errored frame in the signal. This field is only valid if protocol encapsulation is SONET, and monitoring is enabled.
LOF enable	Indicates whether Loss of Frame monitoring is enabled via the **monitor enable** command.
SEF enable	Indicates whether severely errored frame monitoring is enabled via the **monitor enable** command.

The following example shows how to display hardware register information about a transponder wave interface. (See Table 3-8 for field descriptions.)

```
Switch# show controllers wave 3/1
Controller info for Wave interface Wave3/1
  LRC start addr = 0x200000
  hardware port = 2
    RCI1 monitor................:enabled
    port 2 intr SRC/CPU.........:enabled
    CPU0 MSB MAC................:0x0
    CPU0 LSB MAC................:0x0
    CPU1 MSB MAC................:0x0
    CPU1 LSB MAC................:0x0
    port error register.........:0x10000
    port ctrl msg intf mask.....:0xF00FC00A
    port APS port fail mask.....:0x0
  HuJr start addr = 0x250000
  Optics control and status:
    auto fail-over indication...:normal
    optical switch alarm........:clear
    line laser degrade alarm....:clear
    optical switch position.....:Mux 1
    loss of light...............:no
    BLC and LAS.................:disabled
    LSC.........................:disabled
    quick shutdown (FLC)........:disabled
  CDR control and status:
    loss of lock................:yes
    loss of lock enable.........:enabled
  SerDes control and status:
    diags loop back.............:disabled
    line loop back..............:disabled
  GE handler control and status:
    loss of sync................:no
    loss of sync enable.........:disabled
  FC/ESCON handler control and status:
    loss of sync................:no
    loss of sync enable.........:disabled
  SONET handler control and status:
    loss of frame...............:yes
    severely errored frame......:yes
    LOF enable..................:disabled
    SEF enable..................:disabled
```

The following example shows how to display hardware register information about an OSC wave interface. (See Table 3-8 for field descriptions.)

```
Switch# show controllers wave 0
Controller info for OSC wave interface Wave0
  LRC start addr = 0x900000
  hardware port = 0
    RCI0 monitor................:enabled
    port 0 intr SRC/CPU.........:enabled
    CPU0 MSB MAC................:0x0
    CPU0 LSB MAC................:0x1060000
    CPU1 MSB MAC................:0x0
    CPU1 LSB MAC................:0x1070000
    port error register.........:0x8002
    port ctrl msg intf mask.....:0x0
    port APS port fail mask.....:0x0
  HuJr start addr = 0x940000
  CDL add/drop control and status:
    FIFO overflow indication....:clear
    HEC error threshold exceeded:indicate
    FIFO overflow enable........:disabled
    HEC error threshold enable..:disabled
    CDL alarm status............:true alarm
    CDL add enable..............:enabled
    CDL drop enable.............:enabled
  Optics control and status:
    LSC indication..............:ok
    trunk laser failure alarm...:indicated
    LSC indication enable.......:disabled
    trunk laser alarm enable....:disabled
    loss of light...............:yes
    wavelength deviation alarm..:clear
    LSC.........................:disabled
    wavelength select...........:n [hi wlen]
  CDR control and status:
    loss of lock................:yes
    loss of lock enable.........:disabled
  SerDes control and status:
    diags loop back.............:disabled
    network loop back...........:disabled
  GE handler control and status:
    loss of sync................:yes
    loss of sync enable.........:disabled
```

Related Commands	Command	Description
	clear performance history	Specifies the protocol encapsulation for a transparent interface.
	laser control forward enable	Configures forward laser control, which automatically shuts down transponder lasers.
	laser control safety enable	Configures laser safety control on a wave interface.
	laser shutdown	Configures signal loopback on an interface.
	monitor enable	Enables signal monitoring for certain protocol encapsulations.
	show interfaces	Displays interface information.

show interfaces

To display interface information, use the **show interfaces** command.

show interfaces [*type slot*[*/subcard*[*/port*]]]

Syntax Description

type	Specifies one of the interface types listed in Table 3-9.
slot	Specifies a chassis slot.
subcard	Specifies a subcard position in a motherboard.
port	Specifies a port.

Defaults

Displays information for all interfaces on the system.

Command Modes

EXEC and privileged EXEC

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
12.1(10)EV2	Support for 10-GE transponder module was added.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Table 3-9 shows the interface types for the **show interfaces** command.

Table 3-9   Interface Types for the show interfaces Command

Type	Description
fastethernet 0	Shows the NME interface information.
fastethernet-sby 0	Shows the NME interface information for the standby processor card.
filter *slot*/*subcard*/*port*	Shows the filter interface information.
oscfilter *slot*/*subcard*	Shows the OSC oscfilter interface information.
tengigethernetphy *slot*/*subcard*	Shows the tengigethernetphy interface information.

Table 3-9   Interface Types for the show interfaces Command (continued)

Type	Description
thru *slot*/*subcard*	Shows the thru interface information.
transparent *slot*/*subcard*/**0**	Shows the transparent interface information.
wave *slot*[/*subcard*]	Shows the wave interface information.
waveethernetphy *slot*/*subcard*	Shows the waveethernetphy subinterface information.
wavepatch *slot*/*subcard*/*port*	Shows the wavepatch interface information.
wdm *slot*/*subcard*	Shows the wdm interface information.

Examples   The following example shows how to display transparent interface information. (See Table 3-10 for field descriptions.)

```
Switch# show interfaces transparent 3/1/0
Transparent3/1/0 is administratively up, line protocol is up
  Signal quality: Loss of lock
  Encapsulation: Sonet     Rate: oc3
  Signal monitoring: on
  Forward laser control: Off
  Configured threshold Group: None
  Threshold monitored for: BIP1 error
  Set threshold SF:10e-5  SD:10e-7
  Section code violation error count(bip1): 61286
  Number of errored seconds(es): 2
  Number of severely errored seconds(ses): 2
  Number of severely errored framing seconds(sefs): 273
  Number of times SEF alarm raised: 0
  Number of times SF threshold exceeded: 0
  Number of times SD threshold exceeded: 2
  Loopback not set
  Last clearing of "show interface" counters never
Hardware is transparent
```

Table 3-10   show interfaces transparent Field Descriptions

Field	Description
Transparent3/1/0 is administratively up	Shows the interface state, either up or down.
line protocol is up	Shows the state of the line protocol, either up or down.
Signal quality	Shows signal quality.
Encapsulation	Shows the encapsulation for the interface.
Rate	Shows the encapsulation rate—either the configured clock rate or the protocol clock rate, if the protocol supports multiple rates.
Signal monitoring	Shows whether signal monitoring is enabled.
Forward laser control	Shows whether forward laser control is enabled.
Configured threshold group	Shows whether a threshold group has been configured for the interface.
Threshold monitored for	Shows what the threshold group is monitored for.

Table 3-10   *show interfaces transparent Field Descriptions (continued)*

Field	Description
Set threshold	Shows alarm thresholds. The output example shows the alarm thresholds for signal failure (SF) and signal degrade (SD).
Section code violation error count (bip1)	Shows the number of BIP1 errors.
Number of errored seconds (es)	Shows the number of errored seconds.
Number of severely errored seconds (ses)	Shows the number of severely errored seconds.
Number of severely errored framing seconds (sefs)	Shows the number of severely errored framing seconds.
Number of times SEF alarm raised	Shows the number of times the SEF alarm was raised.
Number of times SF threshold exceeded	Shows the number of times the signal failure (SF) threshold was exceeded.
Number of times SD threshold exceeded	Shows the number of times the signal degrade (SD) threshold was exceeded.
Loopback not set	Shows whether loopback is enabled.
Last clearing of "show interface" counters	Shows the last time "show interface" counters were cleared.
Hardware is transparent	Shows the hardware type.

The following example shows how to display wave interface information. (See Table 3-11 for field descriptions.)

```
Switch# show interfaces wave 10/0
Wave10/0 is administratively up, line protocol is up
  Channel: 25   Frequency: 195.1 Thz    Wavelength: 1536.61 nm
  Splitter Protected: Yes
  Receiver power level: -37.30 dBm
  Laser safety control: Off
  Forward laser control: Off
  Osc physical port: No
  Wavelength used for inband management: No
  Configured threshold Group: None
  Section code violation error count(bip1): 0
  Number of errored seconds(es): 29
  Number of severely errored seconds(ses): 29
  Number of severely errored framing seconds(sefs): 0
  Number of times SEF alarm raised: 0
  Number of times SF threshold exceeded: 0
  Number of times SD threshold exceeded: 0
  Loopback not set
  Last clearing of "show interface" counters 4d03h
  Hardware is data_only_port
```

Table 3-11   *show interfaces wave Field Descriptions*

Field	Description
Wave10/0 is administratively up	Shows the interface state, either up or down.
line protocol is up	Shows the state of the line protocol, either up or down.

Table 3-11   show interfaces wave Field Descriptions (continued)

Field	Description
Channel Frequency Wavelength	Shows the channel number, frequency, and wavelength of the wave interface.
Splitter Protected	Shows whether the interface is splitter protected.
Receiver power level	Shows the receiver power level. **Note** This field is not present in the OSC wave interface output.
Laser safety control	Shows whether laser safety control is enabled.
Forward laser control	Shows whether forward laser control is enabled.
Osc physical port	Shows whether the interface is an OSC physical port.
Wavelength used for inband management	Shows whether the interface is used for inband management.
Configured threshold group	Shows whether a threshold group has been configured for the interface.
Loopback not set	Shows whether loopback is enabled.
Last clearing of "show interface" counters	Shows the last time "show interface" counters were cleared.
Hardware is data_only_port	Shows the interface type.

The following example shows how to display wave interface information. (See Table 3-11 for field descriptions.)

```
Switch# show interfaces wave 0
Wave0 is administratively up, line protocol is up
  Channel: 0    Frequency: 191.9 Thz    Wavelength: 1562.23 nm
  Splitter Protected: No
  Laser safety control: Off
  Forward laser control: Off
  Osc physical port: Yes
  Wavelength used for inband management: No
  Configured threshold Group: None
  Loopback not set
  Last clearing of "show interface" counters never
  Hardware is OSC_phy_port
  MTU 1492 bytes, BW 10000000 Kbit, DLY 0 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation SNAP, loopback not set
    CDL receive header error count: 0
  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
     3447 packets input, 269630 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
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
```

```
      0 output buffer failures, 0 output buffers swapped out
```

The following example shows how to display wdm interface information. (See Table 3-12 for field descriptions.)

```
Switch# show interfaces wdm 0/0
Wdm0/0 is up, line protocol is up
 Patched Interface: Thru0/1
 Wdm Hw capability: N/A
 Num of Wavelengths Add/Dropped: 8
 List of Wavelengths: 1, 2, 3, 4, 5, 6, 7, 8,
  Hardware is wavelength_add_drop
```

Table 3-12   show interfaces wdm Field Descriptions

Field	Description
Wdm0/0 is up	Shows the interface state, either up or down.
line protocol is up	Shows the state of the line protocol, either up or down.
Patched Interface:	Shows how the mux/demux modules is optically patched.
Num of wavelengths Add/Dropped:	Shows the number of wavelengths added and dropped.
List of Wavelengths:	Shows list of wavelength channel numbers.
Hardware is wavelength_add_drop	Shows the hardware type.

Related Commands

Command	Description
laser control forward enable	Configures forward laser control on an interface.
laser control safety enable	Configures laser safety control on wave interfaces.
loopback	Configures loopback on an interface.
show controllers	Displays interface controller information.

show optical filter

To display information about the channels supported by the mux/demux modules, use the **show optical filter** command.

show optical filter [**detail**]

Syntax Description

detail	Shows optical patch connections between the mux/demux modules in addition to the channels supported. This information displays only if the patch connection have been configured with the **patch** command.

Defaults

Displays only the channels supported by the mux/demux modules.

Command Modes

EXEC and privileged EXEC

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to verify the channels supported by the mux/demux modules on the system.

Examples

The following example shows how to display optical filter information. (See Table 3-13 for field descriptions.)

```
Switch# show optical filter
aggregate                        filtered
interface         channel(s)     interface
----------------  -----------    -----------
Wdm0/0                0           Oscfilter0/0
Wdm0/0                1           Filter0/0/0
Wdm0/0                2           Filter0/0/1
Wdm0/0                3           Filter0/0/2
Wdm0/0                4           Filter0/0/3
Wdm0/0                5           Filter0/0/4
Wdm0/0                6           Filter0/0/5
```

```
Wdm0/0                    7           Filter0/0/6
Wdm0/0                    8           Filter0/0/7
Wdm0/2                   17           Filter0/2/0
Wdm0/2                   18           Filter0/2/1
Wdm0/2                   19           Filter0/2/2
Wdm0/2                   20           Filter0/2/3
Wdm0/2                   21           Filter0/2/4
Wdm0/2                   22           Filter0/2/5
Wdm0/2                   23           Filter0/2/6
Wdm0/2                   24           Filter0/2/7
Wdm1/0                    0           Oscfilter1/0
Wdm1/0                    1           Filter1/0/0
Wdm1/0                    2           Filter1/0/1
Wdm1/0                    3           Filter1/0/2
Wdm1/0                    4           Filter1/0/3
Wdm1/0                    5           Filter1/0/4
Wdm1/0                    6           Filter1/0/5
Wdm1/0                    7           Filter1/0/6
Wdm1/0                    8           Filter1/0/7
```

Table 3-13   show optical filter Field Descriptions

Field	Description
aggregate interface	Shows the aggregate wdm interface.
channels	Shows the channels in the aggregate interface. In the output example, "remaining" indicates that whichever channels have not been dropped are passed to the thru interface.
filtered interface	Shows the filtered interface, which connects to the transponder.
remaining	Indicates that the channels not supported on the mux/demux modules are passed through to the next mux/demux module.
patched mux/demux interface	Shows the patch connection to another mux/demux module.

The following example shows how to display optical filter information on a shelf with add/drop mux/demux modules. (See Table 3-14 for field descriptions.)

```
Swtich# show optical filter detail
aggregate                          filtered               patched mux/demux
interface         channel(s)       interface              interface
----------------- -----------      -----------------      -----------------
Wdm0/3                  0           Oscfilter0/3
Wdm0/3                 25           Filter0/3/0
Wdm0/3                 26           Filter0/3/1
Wdm0/3                 27           Filter0/3/2
Wdm0/3                 28           Filter0/3/3
Wdm0/3                 29           Filter0/3/4
Wdm0/3                 30           Filter0/3/5
Wdm0/3                 31           Filter0/3/6
Wdm0/3                 32           Filter0/3/7
Wdm0/3            remaining         Thru0/3                Thru1/3
Wdm1/3                  0           Oscfilter1/3
Wdm1/3                 25           Filter1/3/0
Wdm1/3                 26           Filter1/3/1
Wdm1/3                 27           Filter1/3/2
Wdm1/3                 28           Filter1/3/3
Wdm1/3                 29           Filter1/3/4
Wdm1/3                 30           Filter1/3/5
Wdm1/3                 31           Filter1/3/6
```

```
Wdm1/3                32          Filter1/3/7
Wdm1/3                remaining   Thru1/3              Thru0/3
```

Table 3-14   show optical filter detail Field Descriptions

Field	Description
aggregate interface	Shows the aggregate wdm interface.
channels	Shows the channels in the aggregate interface. In the output example, "remaining" indicates that whichever channels have not been dropped are passed to the thru interface.
filtered interface	Shows the filtered interface, which connects to the transponder.
remaining	Indicates that the channels not supported on the mux/demux modules are passed through to the next mux/demux module.
patched mux/demux interface	Shows the patch connection to another mux/demux module.

Related Commands

Command	Description
patch	Configures patch connections for a shelf.
show connect	Displays optical connection information.
show patch	Displays optical patch connection configuration.

show optical interface brief

To display the optical characteristics of all the transponders in the system, use the **show optical interface brief** command.

> **show optical interface brief**

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   EXEC and privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(12c)EV2	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to quickly verify the status of the optical signals on the transponder module interfaces. For more detailed information about the interface, use the **show interfaces** command.

Examples   The following example shows how to display optical interface signal information. (See Table 3-15 for field descriptions.)

```
Switch# show optical interface brief

I Interface      Status/Prot  Laser  Signal Quality   Rx Power     Speed/Encap
-----------      -----------  -----  --------------   -----------  ---------------
Wave0            down/down    on     Loss of light    n/a          SNAP
Wave1            up/up        on     Good             n/a          SNAP
WdmS0/2/0*       down/down    n/a    Loss of light    < -32.00 dBm n/a
WdmS0/2/1        down/down    n/a    Loss of light    < -32.00 dBm n/a
Trans2/2/0       up/up        on     Good             n/a          GigbitEthernet
Wave2/2          up/up        on     Good             -16.78 dBm   n/a
Wavep2/2/0       admin/down   n/a    n/a              Unknown      n/a
Wavep2/2/1*      up/up        n/a    n/a              -16.76 dBm   n/a
```

```
TenGE3/1       up/up       on    Good            n/a            10G Ethernet
Ether3/1/1     up/up       n/a   Good            n/a            SNAP
WaveE3/1       up/up       on    Good            -12.45 dBm     n/a
Ether3/1/0     up/up       n/a   Good            n/a            SNAP
Wavep3/1/0*    up/up       n/a   n/a             -12.45 dBm     n/a
Wavep3/1/1     up/up       n/a   n/a             Unknown        n/a
Trans4/0/0     down/down   on    Loss of light   n/a            916000 KHz
Wave4/0        down/down   on    Loss of light   < -33.00 dBm   n/a
Wavep4/0/0*    down/down   n/a   n/a             < -33.00 dBm   n/a
Trans9/0/0     admin/down  off   n/a             n/a            SONET  oc48
Wave9/0        admin/down  off   n/a             < -35.00 dBm   n/a
Wavep9/0/0*    down/down   n/a   n/a             < -35.00 dBm   n/a
Wavep9/0/1     down/down   n/a   n/a             Unknown        n/a
```

Table 3-15   show optical interface brief Field Descriptions

Field	Description
Interface	Shows the interface identifier.
Status/Prot	Shows the interface status and the protocol status.
Laser	Shows the laser status.
Signal Quality	Shows the current signal quality.
Rx Power	Shows the receiver power.
Speed/Encap	Shows the signal speed or protocol encapsulation for the interface.

Related Commands

Command	Description
show interfaces	Displays system interfaces.

show patch

To display the patch connections, use the **show patch** command.

show patch [**detail**]

Syntax Description	detail	Displays both the user and automatic local path connections.

Defaults   Displays summary patch connection information.

Command Modes   EXEC and privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to display the patch connections on the mux/demux modules configured with the **patch** command.

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

Examples   The following example shows how to display patch connection information. (See Table 3-16 for field descriptions.)

```
Switch# show patch
Patch Interface     Patch Interface     Type        Dir    Error
-----------------   -----------------   ---------   ----   ----------------
Thru0/0             Wdm0/1              USER        Both
Thru0/1             Thru1/0             USER        Both
```

Cisco ONS 15540 ESPx Command Reference Guide

The following example shows how to display detailed patch connection information. (See Table 3-16 for field descriptions.)

```
Switch# show patch detail
Patch Interface    Patch Interface    Type        Error
---------------    ---------------    ---------   -------
Wavepatch10/0/0    Filter0/3/0        AUTOMATIC
Wavepatch10/1/0    Filter0/3/1        AUTOMATIC
Wavepatch10/2/0    Filter0/3/2        AUTOMATIC
Wavepatch10/3/0    Filter0/3/3        AUTOMATIC
Wave0              Oscfilter0/0       USER
Wdm0/0             Thru0/1            USER
Wdm0/1             Thru0/2            USER
Wdm0/2             Thru0/3            USER
Thru0/0            Wdm0/3             USER
```

Table 3-16   show patch detail Field Descriptions

Field	Description
Patch Interface	Shows an interface identifier for the patch connection.
Type	Shows how the patch was configured, either by the system or by the user.
Error	Shows patch errors, such as channel mismatches.

Related Commands

Command	Description
debug ports	Enables debugging of optical port activity.
patch	Configures patch connections within a shelf.

show performance

To display the performance history counters, use the **show performance** command.

show performance {**current** | **history** | **24-hour**} [*interface*] [*interval number*]

Syntax Description

current	Displays the current counter.
history	Displays the 15-minute history counter.
24-hour	Displays the 24-hour counter.
interface	Displays the performance history counter for the specified interface.
interval number	Displays the performance history counter with the specified interval number (1 to 96).

Defaults

Displays all performance history counters (the current counter, all 15-minute history counters, and the 24-hour counter) for all Cisco ONS 15540 ESPx interfaces.

Command Modes

EXEC and privileged EXEC

Command History

This table includes the following release-specific history entry:

SV-Release	Modification
12.2(29)SV	This command was introduced.

Usage Guidelines

Use this command to view the performance history counters for the Cisco ONS 15540 ESPx interfaces.

Examples

The following example shows how to display the current counter for a transparent interface. (See Table 3-17 for field descriptions.)

```
Switch# show performance current transparent 2/2/0
Current 15 minute performance register
-------------------------------------
Interface        : Transparent2/2/0
Interval Number : 81

Elapsed Time(seconds) : 526
Valid Time(seconds)   : 526

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

Table 3-17   *show performance current Field Descriptions*

Field	Description
Interface	Shows the interface for which the current counter is displayed.
Interval Number	Shows the current counter's interval number.
Elapsed Time	Shows the elapsed time since the current counter was started.
Valid Time	Shows the time period during which the interface was administratively up. A current counter with zero valid time will not contain any valid data.
Code violation and running disparity error count	Shows the total number of code violation and running disparity (CVRD) errors in the frames that were received from the client device during the elapsed time of the current performance counter.

The following example shows how to display the 15-minute history counter for a tengigethernetphy interface with CDL disabled. (See Table 3-18 for field descriptions.)

```
Switch# show performance history tengigEthernetPhy 10/0 20
15 minute performance history register
-------------------------------------
Interface        : TenGigEthernetPhy10/0
Interval Number : 20

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

Code violation and running disparity error count : 0
TenGige Non CDL Pkt count  : 0
```

Table 3-18   *show performance history Field Descriptions*

Field	Description
Interface	Shows the interface for which the 15-minute history counter is displayed.
Interval Number	Shows the 15-minute history counter's interval number.
Total Time	Shows the duration of the 15-minute history counter in seconds.
Valid Time	Shows the time period during which the 15-minute history counter was in the no shutdown state. A 15-minute history counter with zero valid time will not contain any valid data.
Code violation and running disparity error count	Shows the total number of CVRD errors in the GE frames that were received from the client interface during the 15 minute period.
TenGige Non CDL Pkt count	Shows the total number of non CDL type packets that were received from the client side during the 15 minute period.

The following example shows how to display the 24-hour counter for a tengigethernetphy interface with CDL enabled. (See Table 3-19 for field descriptions.)

```
Switch# show performance 24-hour tenGigEthernetPhy 10/1
24 hour performance register
----------------------------
Interface        : TenGigEthernetPhy10/1

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

Code violation and running disparity error count : 0
TenGige Non CDL Pkt count  : 0
CDL HEC error count        : 0
TenGige CDL idle Pkt count : 0
```

Table 3-19   show performance 24-hour Field Descriptions

Field	Description
Interface	Shows the interface for which the 24-hour counter is displayed.
Total Time	Shows the duration of the 24-hour counter in seconds.
Valid Time	Shows the time period during which the 24-hour counter was in the no shutdown state. A 24-hour counter with zero valid time will not contain any valid data.
Code violation and running disparity error count	Shows the total number of CVRD errors in the GE frames that were received from the fabric during the 24 hour period.
TenGige Non CDL Pkt count	Shows the total number of non CDL type packets that were received from the client side during the 24 hour period.
CDL HEC error count	Shows the total number of GE frames that were received with CDL HEC errors during the 24 hour period.
TenGige CDL idle Pkt count	Shows the total number of CDL idle packets that were received from the client during the 24 hour period.

Related Commands

Command	Description
show interfaces	Displays interface information.
auto-sync counters interface	Enables the automatic synchronization of the performance history counters.
clear performance history	Clears the performance history counters.

shutdown

To disable an interface, use the **shutdown** command. To restart a disabled interface, use the **no** form of this command.

shutdown

no shutdown

Syntax Description   This command has no other arguments or keywords.

Defaults   Disabled

Command Modes   Interface configuration

Usage Guidelines   This command disables all functions on the specified interface.

This command also marks the interface as unavailable. To check whether an interface is disabled, use the **show interfaces** command. An interface that has been shut down is shown as administratively down in the **show interfaces** output.

On transparent and wave interfaces, use the **shutdown** command to turn off the transmit lasers. To turn the transmit lasers on, use the **no shutdown** command.

On CDL capable interfaces, such as tengigethernetphy and waveethernetphy interfaces, use the **shutdown** command to stop sending data traffic. To resume sending data traffic, use the **no shutdown** command. On the 10-GE transponder module, use the **laser shutdown** command to turn the lasers off and on.

A **shutdown** command issued on a wave interface does not affect administrative status of the corresponding wavepatch interfaces. To administratively shut down the wavepatch interfaces, issue **shutdown** commands directly.

To use splitter protected line card motherboards for line card protection, you must shut down all the wavepatch interfaces connected to one of the mux/demux motherboards. (See the "Examples" section.)

The **laser shutdown** command does not affect the function of the **shutdown** command.

Examples   The following example shows how to shut down a wave interface, which also turns off the laser that transmits to the trunk fiber.

```
Switch# configure terminal
Switch(config)# interface wave0/3
Switch(config-if)# shutdown
```

The following example shows how to reenable a transparent interface and turn on the laser transmitting to the client equipment.

```
Switch# configure terminal
Switch(config)# interface transparent 8/0/0
Switch(config-if)# no shutdown
```

The following example shows how to disable the east (slot 1) side of the wavepatch interface pair on a splitter protected line card motherboard.

```
Switch# configure terminal
Switch(config)# interface wavepatch 3/0/1
Switch(config-if)# shutdown
```

Related Commands

Command	Description
laser shutdown	Turns off a laser.
show interfaces	Displays system interfaces.

C H A P T E R **4**

Online Diagnostics Commands

Online diagnostics test the accessibility of the components on the Cisco ONS 15540 ESPx. Use the following commands to configure and monitor online diagnostic operations.

diag online

To enable online diagnostics for the system, use the **diag online** command. To disable online diagnostics for the system, use the **no** form of this command.

> **diag online**

> **no diag online**

Syntax Description   This command has no other arguments or keywords.

Defaults   Disabled

Command Modes   Global configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to enable or disable online diagnostics for the system. Online diagnostics run in background mode or during OIR (online insertion and removal). Any slot level diagnostics previously configured with the**diag online slot** command take precedence over the **diag online** command.

When online diagnostics are disabled, no further diagnostics can run.

Examples   The following example shows how to enable online diagnostics.

```
Switch# configure terminal
Switch(config)# diag online
```

Related Commands	Command	Description
	debug diag online	Enables debugging of the online diagnostics.
	diag online slot	Enables online diagnostics for a specified slot number.
	diag online subslot	Enables online diagnostics for a specified subslot number.
	show diag online	Displays the configuration and status of the online diagnostics.
	show diag online detail	Shows detailed online diagnostic test results for the shelf.
	show diag online slot	Shows detailed online diagnostic test results for a specific slot.

diag online slot

To enable online diagnostics for a specified slot number, use the **diag online slot** command. To disable online diagnostics for a specified slot number, use the **no** form of this command.

> **diag online slot** *slot-number* [**timer** *seconds*]

> **no diag online slot** *slot-number* [**timer** *seconds*]

Syntax Description

slot-number	Specifies the number of the slot on which to run online diagnostics. The range is 0 to 11.
timer *seconds*	Specifies a timer the background tests. The range is 30 to 600 seconds. The default value is 60 seconds.

Defaults

Disabled.

The timer default is 60 seconds.

Command Modes

Global configuration

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
12.1(12c)EV	The timer option was added.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to enable or disable online diagnostics for a specified slot number. It can be useful to disable online diagnostics on a particular slot when there is a spurious error that causes excessive console messages.

Examples

The following example shows how to enable online diagnostics for a specific slot number.

```
Switch# configure terminal
Switch(config)# diag online subslot 2
```

The following example shows how to enable online diagnostics on all the slots and then disable online diagnostics for a specific slot number.

```
Switch# configure terminal
Switch(config)# diag online
Switch(config)# no diag online subslot 10
```

Related Commands	**Command**	**Description**
	debug diag online	Enables debugging of the online diagnostics.
	diag online	Enables online diagnostics for the system.
	diag online subslot	Enables online diagnostics for a specified subslot number.
	show diag online	Displays the configuration and status of the online diagnostics.
	show diag online detail	Shows detailed online diagnostic test results for the shelf.
	show diag online slot	Shows detailed online diagnostic test results for a specific slot.

diag online subslot

To enable online diagnostics for a specified subslot number, use the **diag online subslot** command. To disable online diagnostics for a specific slot number, use the **no** form of this command.

diag online subslot *slot*/*subcard* [**timer** *seconds*]

no diag online subslot *slot*/*subcard* [**timer** *seconds*]

Syntax Description		
slot	Specifies the number of the slot on which to run online diagnostics. The range is 0 to 11.	
subcard	Specifies the number of the subslot on which to run online diagnostics. The range is 0 to 1.	
timer *seconds*	Specifies a timer the background tests. The range is 30 to 600 seconds. The default value is 60 seconds.	

Defaults

Disabled.

The timer default is 60 seconds.

Command Modes

Global configuration

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(12c)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to enable or disable online diagnostics for a specific subslot.

You can disable online diagnostics on a particular subslot when there is a spurious error that causes excessive console messages.

Examples

The following example shows how to enable online diagnostics for a specific slot number.

```
Switch# configure terminal
```

```
Switch(config)# diag online subslot 0/0
```

The following example shows how to enable online diagnostics on all the slots and then disable online diagnostics for a specific slot number.

```
Switch# configure terminal
Switch(config)# diag online
Switch(config)# no diag online subslot 0/1
```

	Command	Description
Related Commands	debug diag online	Enables debugging of the online diagnostics.
	diag online	Enables online diagnostics for the system.
	diag online slot	Enables online diagnostics for specified slot number.
	diag online subslot	Enables online diagnostics for a specified subslot number.
	show diag online	Displays the configuration and status of the online diagnostics.
	show diag online detail	Shows detailed online diagnostic test results for the shelf.
	show diag online slot	Shows detailed online diagnostic test results for a specific slot.

show diag online

To display current online diagnostic test results, use the **show diag online** command. Information displayed includes the cards installed, their current status, and the status of online tests performed on the cards.

show diag online

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   EXEC and privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command whenever a card is unavailable or is not coming up, to determine card status and the status of various background online tests performed on them.

Examples   The following example shows how to display online diagnostic test results for the hardware components. (See Table 4-1 for field descriptions.)

```
Switch# show diag online
Online Diagnostics Current Summary Information
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
On ACTIVE CPU card Slot: 6
CPU Uptime:    21 hours, 52 minutes

 Slot       CardType        Enabled    Bootup/     Periodic     Previous
                                       Insertion   Background   Failures
                                       tests       tests

 ~~~~~~     ~~~~~~~~~~~~~~   ~~~~~~~    ~~~~~~~~~    ~~~~~~~~~~   ~~~~~~~~
 0/*/*      Mx-DMx-Mthrbd    Yes       Pass         Pass          No
```

```
    0/ 3/*Mx-DMx-8Mod-Plus1-W        Yes     Pass        Pass        No

    1/*/*      Mx-DMx-Mthrbd         Yes     Pass        Pass        No
    1/ 3/*Mx-DMx-8Mod-Plus1-W        Yes     Pass        Pass        No

    6/*/*         Queens CPU         Yes     Pass        Pass        No

    7/*/*         Queens CPU         Yes     Pass        Pass        No

   10/*/*   XpndrMotherboard         Yes     Pass        Pass        No
   10/ 0/*  NPlugXpndrMonitor        Yes     Pass        Pass        No
   10/ 1/*  NPlugXpndrMonitor        Yes     Pass        Pass        No
   10/ 2/*  NPlugXpndrMonitor        Yes     Pass        Pass        No
   10/ 3/*  NPlugXpndrMonitor        Yes     Pass        Pass        No
```

Table 4-1   show diag online Field Descriptions

Field	Description
Slot	Shows the slot on which online diagnostics have been run.
CardType	Shows the card type on which online diagnostics have been run. Card types include: • Mx-DMx-Mthrbd (Mux/demux motherboard) • Mx-DMx-8Mod-Plus1-W (8-channel mux/demux module with OSC) • XpndrMotherboard (Line card motherboard) • NPlugXpndrMonitor (Transponder module) • Queens CPU (Processor card)
Enabled	Indicates whether online diagnostic tests are enabled on the slot.
Bootup/Insertion tests	Indicates whether the card passed the test run at system bootup or when the component is inserted in the chassis.
Periodic Background tests	Indicates whether the card passed the periodic background tests.
Previous Failures	Shows when the last failure occurred for the component.

Related Commands

Command	Description
diag online	Enables online diagnostics for the system.
diag online slot	Enables online diagnostics for the specified slot.
show diag online detail	Shows detailed online diagnostic test results for the shelf.
show diag online slot	Shows detailed online diagnostic test results for a specific slot.

show diag online detail

To display the cards currently installed on the system and the detailed results of online diagnostic tests performed on them, use the **show diag online detail** command.

show diag online detail

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   EXEC and privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to display detailed status information about all the online diagnostic tests run on the hardware in the system. Information displayed includes the number of times background tests passed or failed, as well as the status of OIR tests.

Use this command to debug possible hardware problems on the cards or subcards installed.

Examples   The following example shows how to display current, detailed online diagnostics for the system. (See Table 4-2 for field descriptions.)

```
Switch# show diag online detail

Online Diagnostics Detailed Information
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
On ACTIVE CPU card Slot: 6
CPU Uptime:    21 hours, 57 minutes

_____
Slot[0]:Mx-DMx-Mthrbd
```

```
Enabled: Yes

Online Insertion Tests
  Slot         CardType        TestType      Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
  0/*/*      Mx-DMx-Mthrbd    lrcAccess      Pass    0 minutes      never
                             idpromAccess    Pass
  0/ 3/* Mx-DMx-8Mod-Plus1- idpromAcces     Pass    0 minutes      never

Online Background Tests
  Slot         CardType        TestType      Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
  0/*/*      Mx-DMx-Mthrbd    lrcAccess      Pass21 hours, 57      never
                             idpromAccess    Pass
  0/ 3/* Mx-DMx-8Mod-Plus1- idpromAcces     Pass21 hours, 57      never
_____
Slot[1]:Mx-DMx-Mthrbd
Enabled: Yes

Online Insertion Tests
  Slot         CardType        TestType      Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
  1/*/*      Mx-DMx-Mthrbd    lrcAccess      Pass    0 minutes      never
                             idpromAccess    Pass
  1/ 3/* Mx-DMx-8Mod-Plus1- idpromAcces     Pass    0 minutes      never

Online Background Tests
  Slot         CardType        TestType      Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
  1/*/*      Mx-DMx-Mthrbd    lrcAccess      Pass21 hours, 57      never
                             idpromAccess    Pass
  1/ 3/* Mx-DMx-8Mod-Plus1- idpromAcces     Pass21 hours, 57      never
_____
Slot[6]:Queens CPU
Enabled: Yes

Online Insertion Tests
  Slot         CardType        TestType      Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
  6/*/*       Queens CPU     srcStatus      Pass    0 minutes      never
                             PCIAccess       Pass
  Slot         CardType        TestType      Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
                             PCMCIAAccess    Pass

Online Background Tests
  Slot         CardType        TestType      Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
  6/*/*       Queens CPU     srcStatus      Pass21 hours, 57      never
                             PCIAccess       Pass
                             PCMCIAAccess    Pass
_____
Slot[7]:Queens CPU
Enabled: Yes

Online Insertion Tests
  Slot         CardType        TestType      Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
  7/*/*       Queens CPU     srcStatus      Pass    0 minutes      never
                             PCIAccess       Pass
                             PCMCIAAccess    Pass

Online Background Tests
  Slot         CardType        TestType      Status   LastRunTime   LastFailTime
```

```
 ~~~~~~   ~~~~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
 7/*/*         Queens CPU    srcStatus     Pass21 hours, 51      never
                             PCIAccess     Pass
                             PCMCIAAccess  Pass
_____
Slot[10]:XpndrMotherboard
Enabled: Yes

Online Insertion Tests
 Slot          CardType        TestType     Status    LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
10/*/*   XpndrMotherboard    lrcAccess     Pass     0 minutes      never
                             idpromAccess  Pass
10/ 0/*  NPlugXpndrMonitor   scAccess      Pass     0 minutes      never
                             idpromAcces   Pass
10/ 1/*  NPlugXpndrMonitor   scAccess      Pass     0 minutes      never
                             idpromAcces   Pass
10/ 2/*  NPlugXpndrMonitor   scAccess      Pass     0 minutes      never
                             idpromAcces   Pass
10/ 3/*  NPlugXpndrMonitor   scAccess      Pass     0 minutes      never
                             idpromAcces   Pass

Online Background Tests
 Slot          CardType        TestType     Status    LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
10/*/*   XpndrMotherboard    lrcAccess     Pass21 hours, 57      never
                             idpromAccess  Pass
 Slot          CardType        TestType     Status    LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
10/ 0/*  NPlugXpndrMonitor   scAccess      Pass21 hours, 57      never
                             idpromAcces   Pass
10/ 1/*  NPlugXpndrMonitor   scAccess      Pass21 hours, 57      never
                             idpromAcces   Pass
10/ 2/*  NPlugXpndrMonitor   scAccess      Pass21 hours, 57      never
                             idpromAcces   Pass
10/ 3/*  NPlugXpndrMonitor   scAccess      Pass21 hours, 57      never
                             idpromAcces   Pass
```

Table 4-2   show diag online detail Field Descriptions

Field	Description
On ACTIVE CPU card Slot:	Shows the chassis slot that contains the active processor card.
CPU Uptime	Shows the amount of time since the system booted.
Slot	Shows the slot on which the online diagnostics are being run.
Enabled	Indicates whether online diagnostics are enabled on the slot.
CardType	Shows the card type on which the online diagnostics are being run. Card types include: • Mx-DMx-Mthrbd (Mux/demux motherboard) • Mx-DMx-8Mod-Plus1-W (8-channel mux/demux module with OSC) • XpndrMotherboard (Line card motherboard) • NPlugXpndrMonitor (Transponder module) • Queens CPU (Processor card)

Table 4-2   show diag online detail Field Descriptions (continued)

Field	Description
TestType	Shows the type of test run. Test types can be: • lrcAccess (Accesses the LRC) • idpromAccess (Accesses the IDPROM) • srcAccess (Accesses the SRC) • PCMCIAAccess (Accesses Flash PC Cards • scAccess (Accesses transponder modules)
Status	Shows the result of the diagnostic test (Pass/Fail).
LastRunTime	Shows the amount of time since the test was last run.
LastFailTime	Shows the amount of time since the test failed.

Related Commands

Command	Description
diag online	Enables online diagnostics for the system.
diag online slot	Enables online diagnostics for the specified slot.
diag online subslot	Enables online diagnostics for a specified subslot number.
show diag online	Shows a summary of the online diagnostic test results for the shelf.
show diag online slot	Shows detailed online diagnostic test results for a specific slot.

show diag online slot

To display the results of online diagnostic tests performed on a card in a specific slot, use the **show diag online slot** command.

show diag online slot *slot-number*

Syntax Description

slot-number	Specifies the slot number. The range is 0 to 11.

Defaults

None

Command Modes

EXEC and privileged EXEC

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to display the status of online diagnostics performed on components installed in a specific slot.

Examples

The following example shows how to display the results of online diagnostic tests performed on slot 0. (See Table 4-3 for field descriptions.)

```
Switch# show diag online slot 0
Online Diagnostics Information Per Slot
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Slot[0]:Mx-DMx-Mthrbd
Enabled: Yes
CPU Uptime:    21 hours, 59 minutes

Online Insertion Tests
 Slot         CardType        TestType      Status    LastRunTime    LastFailTime
 ~~~~~~    ~~~~~~~~~~~~~~~    ~~~~~~~~~    ~~~~~~    ~~~~~~~~~~~    ~~~~~~~~~~~~~~
 0/*/*      Mx-DMx-Mthrbd    lrcAccess      Pass    0 minutes       never
                             idpromAccess   Pass
```

```
0/ 3/* Mx-DMx-8Mod-Plus1- idpromAcces     Pass    0 minutes      never

Online Background Tests
 Slot        CardType        TestType     Status   LastRunTime    LastFailTime
~~~~~~   ~~~~~~~~~~~~~~   ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~~
0/*/*       Mx-DMx-Mthrbd   lrcAccess     Pass21 hours, 58      never
                        idpromAccess    Pass
0/ 3/* Mx-DMx-8Mod-Plus1- idpromAcces     Pass21 hours, 58      never
```

Table 4-3   show diag online slot Field Descriptions

Field	Description
Slot	Shows the slot on which online diagnostics were performed.
Enabled	Indicates whether online diagnostics are enabled on the slot.
CPU Uptime	Shows the amount of time since the system booted.
CardType	Shows the card type on which the online diagnostics are being run. Card types include: • Mx-DMx-Mthrbd (Mux/demux motherboard) • Mx-DMx-8Mod-Plus1-W (8-channel mux/demux module with OSC) • XpndrMotherboard (Line card motherboard) • NPlugXpndrMonitor (Transponder module) Queens CPU (Processor card)
TestType	Shows the type of test run. Test types can be: • lrcAccess (Accesses the LRC) • idpromAccess (Accesses the IDPROM) • srcAccess (Accesses the SRC) • PCMCIAAccess (Accesses Flash PC Cards) • scAccess (Accesses transponder modules)
Status	Shows the result of the diagnostic test (Pass/Fail).
LastRunTime	Shows the amount of time since the test was last run.
LastFailTime	Shows the amount of time since the test failed.

Related Commands

Command	Description
diag online	Enables online diagnostics for the system.
diag online slot	Enables online diagnostics for the specified slot.
diag online subslot	Enables online diagnostics for a specified subslot number.
show diag online	Shows a summary of the online diagnostic test results for the shelf.
show diag online detail	Shows detailed online diagnostic test results for the shelf.

■   **show diag online slot**

5

OSCP Commands

OSCP (Optical Supervisory Channel Protocol) provides out-of-band network management over a 33rd channel. Use the following commands to configure and monitor OSCP operations.

clear oscp

To clear OSCP statistics or traffic counters, use the **clear oscp** command.

clear oscp {**statistics** | **traffic**}

Syntax Description	statistics	Clears OSCP statistics that can be used to debug the protocol, for example:
		• The hold-down count statistic specifies how many times a hold down has been applied to avoid excessive generation of OSCP Hello packets.
		• The Hello Tx and Rx statistics indicate the number of Hello packets that have been transmitted and received at an interface.
		• The OSCP go-down statistic indicates the number of times an interface has gone out of the two-way state.
	traffic	Clears OSCP control-traffic counters that indicate the number of different protocol packets that were transmitted over the optical supervisory channel.

Defaults   None

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to perform a one-time clear of the specified OSCP statistics or traffic tables. This command is useful for debugging or monitoring OSCP performance.

Examples   The following example shows how to clear OSCP statistics and traffic tables.

```
Switch# clear oscp statistics
Switch# clear oscp traffic
```

Related Commands	Command	Description
	show oscp statistics	Displays OSCP Hello statistics information.
	show oscp traffic	Display OSCP Hello traffic information.

oscp timer hello holddown

To modify the OSCP timer Hello hold-down interval, use the **oscp timer hello holddown** command. To return the Hello hold-down interval to its default value, use the **no** form of the command.

oscp timer hello holddown *milliseconds*

no oscp timer hello holddown

Syntax Description

milliseconds	Specifies, in milliseconds, the interval in which no more than one Hello packet can be generated. If more than one Hello packet is generated during the hold-down period, the extra packets are delayed. The range is 150 to 30000 milliseconds.

Defaults   3000 milliseconds

Command Modes   Global configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to control the amount of OSCP Hello activity that is generated on the network. 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 ensure proper functioning of the OSCP, the Hello hold-down timer value can be no more that 75% of the OSCP Hello interface timer.

Note   There is a trade-off between the frequency of generating Hello packets and the speed in which the system detects that the OSCP has gone down. In certain OSCP failure scenarios, a shorter Hello interval leads to faster detection of the OSCP failure.

Examples   The following example shows how to configure the OSCP timer Hello hold-down interval.

```
Switch# configure terminal
Switch(config)# oscp timer hello holddown 300
```

Related Commands

Command	Description
debug oscp	Enables debugging of OSCP activity.
oscp timer hello interval	Modifies the OSCP timer Hello interval.
oscp timer inactivity-factor	Modifies the OSCP timer inactivity factor.
show oscp info	Displays OSCP configuration information.

oscp timer hello interval

To modify the OSCP timer Hello interval, use the **oscp timer hello interval** command. To return the Hello interval to its default value, use the **no** form of the command.

oscp timer hello interval *milliseconds*

no oscp timer hello interval

Syntax Description

milliseconds	Specifies, in milliseconds, the periodic generation of OSCP Hello packets. The range is 100 to 10000 milliseconds.

Defaults   100 milliseconds

Command Modes   Global configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to control how often OSCP Hello messages are sent. 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.

Note   There is a trade-off between the frequency of generating Hello packets and the speed in which the system detects that the OSCP has gone down. In certain OSCP failure scenarios, a shorter Hello interval leads to faster detection of the OSCP failure.

Examples   The following example shows how to configure the OSCP timer Hello interval.

```
Switch# configure terminal
```

```
Switch(config)# oscp timer hello interval 200
```

Related Commands	Command	Description
	debug oscp	Enables debugging of OSCP activity.
	oscp timer hello holddown	Modifies the OSCP timer Hello hold-down interval.
	oscp timer inactivity-factor	Modifies the OSCP timer Hello inactivity factor.
	show oscp info	Displays OSCP configuration information.

oscp timer inactivity-factor

To modify the OSCP timer Hello inactivity factor, use the **oscp timer inactivity-factor** command. To return the Hello inactivity factor to its default value, use the **no** form of the command.

oscp timer inactivity-factor *factor*

no oscp timer inactivity-factor

Syntax Description

factor	Specifies a value used to calculate an inactivity interval. The specified interval of time is equal to the inactivity factor multiplied by the neighbor's advertised Hello interval. The range is 1 to 50.

Defaults

5 seconds

Command Modes

Global configuration

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines

The system uses this attribute to determine when a neighbor node, or the link to it, has gone down. The link to a neighbor node is considered inactive if an OSCP Hello packet is not received for a time interval determined by the inactivity factor. The time interval is calculated by multiplying the inactivity factor by the advertised hold-down interval. For example, if the neighbor node's advertised hold-down interval is 5 seconds and the local node's inactivity factor is 5, the time interval that the local node will wait until declaring the neighbor node down is 25 seconds.

Note   There is a trade-off between the frequency of generating Hello packets and the speed in which the system detects that the OSCP has gone down. In certain OSCP failure scenarios, a shorter Hello interval leads to faster detection of the OSCP failure.

Examples   The following example shows how to set the OSCP timer Hello inactivity factor to 3.

```
Switch# configure terminal
Switch(config)# oscp timer inactivity-interval 3
```

Related Commands

Command	Description
debug oscp	Enables debugging of OSCP activity.
oscp timer hello holddown	Modifies the OSCP timer Hello hold-down interval.
oscp timer hello interval	Modifies the OSCP timer Hello interval.
show oscp info	Displays OSCP configuration information.

show oscp info

To display OSCP (Optical Supervisory Channel Protocol) configuration information, use the **show oscp info** command.

show oscp info

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   EXEC and privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to display OSCP configuration information for the system.

Examples   The following example shows how to display OSCP configuration information for the system. (See Table 5-1 for field descriptions.)

```
Switch# show oscp info
OSCP protocol version 1, Node ID        0000.1644.28fb
No. of interfaces 1, No. of neighbors 1
Hello interval 50 tenth of sec, inactivity factor 5,

Hello hold-down 1 tenth of sec
Supported OSCP versions: newest 1, oldest 1
```

Table 5-1   show oscp info Field Descriptions

Field	Description
OSCP protocol version	Shows the OSCP version.
Node ID	Shows the node ID.
No. of interfaces	Shows the number of interfaces.
No. of neighbors	Shows the number of neighbors.
Hello interval	Shows the Hello interval in milliseconds.
inactivity factor	Shows the inactivity factor. The system uses the inactivity factor to determine when a link has gone down. A link is returned to the "attempt" state if the system has not received an OSCP Hello packet for a certain time interval. That time interval is equal to the Hello inactivity factor multiplied by the Hello interval from the Hello packet most recently received from the remote system. The range of inactivity factors is from 2 to 50. The default inactivity factor is 5.
Hello hold-down	Shows, in milliseconds, how long to wait before sending another OSCP Hello packet. This avoids excessive generation of OSCP Hello packets.
Supported OSCP versions	Shows the OSCP versions supported.

Related Commands

Command	Description
oscp timer hello holddown	Modifies the OSCP timer Hello hold-down interval.
oscp timer hello interval	Modifies the OSCP timer Hello interval.
oscp timer inactivity-factor	Modifies the OSCP timer inactivity factor.

show oscp interface

To display OSCP (Optical Supervisory Channel Protocol) status information for OSC wave interfaces and ethernetdcc interfaces, use the **show oscp interface** command.

show oscp interface [**wave** *slot*/*subcard* | **ethernetdcc** *slot*/*subcard*/*port*]

Syntax Description	
wave *slot*	Specifies an OSC wave interface.
ethernetdcc *slot*/*subcard*/*port*	Specifies an ethernetdcc interface on a 10-GE transponder module.

Defaults   Displays OSCP status information for all OSC wave interfaces and ethernetdcc interfaces in the system.

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV2	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to display status information for the local and remote interfaces running OSCP.

Examples   The following example shows how to display status information for the local and remote interfaces running OSCP. (See Table 5-2 for field descriptions.)

```
Switch# show oscp interface
Codes: OSC - dedicated wavelength channel, CDL - in-band wavelength channel

OSCP Interface(s)
Local Port          Port ID   Type  OSCP St  Rem Port ID  Rem Node Id
~~~~~~~~~~~~~~~~~~~ ~~~~~~~~  ~~~~  ~~~~~~~  ~~~~~~~~~~~  ~~~~~~~~~~~~~~~
Wave0               02000000  OSC   down     00000000     0000.0000.0000
Wave1               02020000  OSC   down     00000000     0000.0000.0000
```

Table 5-2   ***show oscp interface Field Descriptions***

Field	Description
Local Port	Shows the local port for the OSCP interface.
Port ID	Shows the port ID for the local port.
Type	Shows the channel link type, either OSCP or CDL.
OSCP St	Shows the OSCP Hello state. Valid values are: • down—the physical layer is down • attempt—the physical layer is up, but no Hello messages have been received from the neighbor • 1way—Hello messages have been received from the neighbor, but their content indicates that the neighbor has not yet received Hellos from this node. • 2way—Hello messages have been received from the neighbor indicating that the neighbor has received Hello packets from this node.
Rem Port Id	Shows the port ID for the remote port.
Rem Node Id	Shows the node ID for the remote port.

Related Commands

Command	Description
show oscp neighbor	Displays OSCP neighbor information.
show oscp statistics	Displays OSCP activity statistics.
show oscp traffic	Displays OSCP message traffic information.

show oscp neighbor

To display OSCP (Optical Supervisory Channel Protocol) neighbor information, use the **show oscp neighbor** command.

show oscp neighbor

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   EXEC and privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to display information about the identity of the neighbors communicating with the system through OSCP.

Examples   The following example shows how to display information about the identity of the neighbors communicating with the system through OSCP. (See Table 5-3 for field descriptions.)

```
Switch# show oscp neighbor
OSCP Neighbors
   Neighbor Node Id: 0000.1644.28ff   Port list:
    Local Port     Port ID  Rem Port ID OSCP state
   ~~~~~~~~~~~~~~ ~~~~~~~~~ ~~~~~~~~~~~~ ~~~~~~~~~
    Wave0          1000000  1000000      2way
```

Table 5-3   *show oscp neighbor Field Descriptions*

Field	Description
Neighbor Node Id	Shows the node ID for the OSCP neighbor.
Port list	Shows ports and port IDs for local and remote ports.
Local Port	Shows the local port.
Port Id	Shows the port ID of the local port.
Rem Port ID	Shows the port ID of the remote port.
OSCP St	Shows the OSCP Hello state. Valid values are: • down—the physical layer is down • attempt—the physical layer is up, but no Hello messages have been received from the neighbor • 1-way—Hello messages have been received from the neighbor, but their content indicates that the neighbor has not yet received Hellos from this node. • 2-way—Hello messages have been received from the neighbor indicating that the neighbor has received Hello packets from this node.

Related Commands

Command	Description
show oscp interface	Displays OSCP information for an interface.
show oscp statistics	Displays OSCP activity statistics.
show oscp traffic	Displays OSCP message traffic information.

show oscp statistics

To display OSCP (Optical Supervisory Channel Protocol) Hello statistics, use the **show oscp statistics** command.

> **show oscp statistics** [**wave** *slot*]

Syntax Description

wave *slot*	Specifies an OSC wave interface.

Defaults   Displays OSCP statistics for all OSC wave interfaces in the system.

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to display OSCP Hello statistics for an OSC interface.

This command displays the following OSCP statistics, which can be used to debug the OSCP.

- hold down—Shows how many times a hold down has been applied to avoid excessive generation of OSCP Hello packets.
- Hello Tx pkts and Hello Rx pkts—Shows the number of OSCP Hello packets that have been transmitted to and received at an interface.
- OSCP go down—Shows the number of times an OSC interface has gone out of two-way state.

Examples   The following example shows how to display OSCP control statistics for an OSC interface. (See Table 5-4 for field descriptions.)

```
Switch# show oscp statistics wave 0
OSCP Hello Statistics:

interface Wave0
```

```
 Event                Count
~~~~~~~~~~~~          ~~~~~~~~~~
hold down             3
Hello Tx pkts         2262
Hello Rx pkts         2259
Hello discards in     0
Hello discards out    0
OSCP go down events   2

 Event                Time (seconds)
~~~~~~~~~~~~~~~~~~~~~  ~~~~~~~~~~
Next Tx Hello due     2
Last Hello sent       2
Last Hello received   4
Inactivity interval   25.0
Time until port dropped 20
```

Table 5-4   show oscp statistics Field Descriptions

Field	Description
hold down	Shows how many times a hold down has been applied to avoid excessive generation of OSCP Hello packets.
Hello Tx pkts	Shows the number of Hello transmissions that have been sent.
Hello Rx pkts	Shows the number of Hello transmissions that have been received.
Hello discards in	Shows the number of incoming Hello transmissions that have been discarded.
Hello discards out	Shows the number of outgoing Hello transmissions that have been discarded.
OSCP go down events	Shows the number of times that the OSCP (Optical Supervisory Channel Protocol) has gone down.
Next Tx Hello due	Shows the number of seconds before the next transmit Hello packet is due.
Last Hello sent	Shows the number of seconds since a Hello packet was sent.
Last Hello received	Shows the number of seconds since a Hello packet was received.
Inactivity interval	Shows the number of seconds for the inactivity interval.
Time until port dropped	Shows the number of seconds allowed until the port is dropped.

Related Commands

Command	Description
oscp timer hello holddown	Modifies the OSCP timer Hello hold-down interval.
oscp timer hello interval	Modifies the OSCP timer Hello interval.

show oscp traffic

To display OSCP (Optical Supervisory Channel Protocol) Hello message traffic information, use the **show oscp traffic** command.

show oscp traffic [**wave** *slot*]

Syntax Description

wave *slot*	Specifies an OSC wave interface.

Defaults

Displays OSCP Hello message traffic information for all OSC wave interfaces in the system.

Command Modes

Privileged EXEC

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to display OSCP control traffic statistics, which show the count of different protocol packets that have been transmitted over the optical supervisory channel.

Examples

The following example shows how to display OSCP control traffic statistics, which show the count of different protocol packets that have been transmitted over the optical supervisory channel. (See Table 5-5 for field descriptions.)

```
Switch# show oscp traffic wave 0
OSC Traffic Statistics:

interface Wave0
Description        Count
~~~~~~~~~~~~       ~~~~~~~~~~
Tx IP pkt          0
Rx IP pkt          0
Tx CDP pkt         198
Rx CDP pkt         195
Rx pkt dropped     0
```

Table 5-5   *show oscp traffic Field Descriptions*

Field	Description
Tx IP pkt	Shows number of IP packets that have been transmitted over the optical supervisory channel.
Rx IP pkt	Shows number of IP packets that have been received over the optical supervisory channel.
Tx CDP pkt	Shows number of CDP packets that have been transmitted over the optical supervisory channel.
Rx CDP pkt	Shows number of CDP packets that have been received over the optical supervisory channel.
Rx pkt dropped	Shows the number of receive packets that were dropped.

Related Commands

Command	Description
clear oscp	Clears OSCP statistics or traffic counters.

show oscp traffic

Processor Card Redundancy Commands

Processor card redundancy provides protection against processor card failure. Use the following commands to configure and monitor processor card redundancy operations.

auto-sync counters interface

To enable automatic synchronizing of traffic statistics, performance monitoring counters, and performance history counters on the active processor card to the standby processor card, use the **auto-sync counters interface** command. To disable automatic synchronizing of traffic statistics and performance monitoring counters, use the **no** form of this command.

> **auto-sync counters interface**

> **no auto-sync counters interface**

Syntax Description   This command has no other arguments or keywords.

Defaults   Enabled

Command Modes   Redundancy configuration

Command History   This table includes the following release-specific history entries:

SV-Release	Modification
12.2(24)SV	This command was introduced.
12.2(29)SV	Added support for the automatic syncing of performance history counters.

Usage Guidelines   Use this command to enable or disable automatic synchronizing of the traffic statistics, performance monitoring counters, and performance history counters without affecting the following types of synchronization:

- • Startup configuration

- • Dynamic database synchronizing

- • Running configuration

Examples   The following example shows how to disable automatic synchronizing of the traffic statistics and performance monitoring counters.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# no auto-sync counters interface
```

Related Commands

Command	Description
auto-sync startup-config	Selectively enables only automatic synchronizing of the startup configuration to the standby processor card.
maintenance-mode	Disables all processor card redundancy synchronization.
redundancy	Enters redundancy configuration mode.
redundancy manual-sync	Causes an immediate one-time database update.
show redundancy summary	Displays processor card redundancy status and configuration information.
show redundancy capability	Displays capabilities of the active and standby processor card.

auto-sync running-config

To selectively enable only automatic synchronizing of the running configuration on the active processor to the standby processor card, use the **auto-sync running-config** command. To disable automatic synchronizing of the running configuration, use the **no** form of this command.

auto-sync running-config

no auto-sync running-config

Syntax Description   This command has no other arguments or keywords.

Defaults   Enabled

Command Modes   Redundancy configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to enable or disable automatic synchronizing of the running configuration without affecting the following types of synchronization:

- Startup configuration
- Dynamic database synchronizing

When a processor card switchover occurs, the standby processor card normally uses the running configuration rather than the startup configuration. However, if **auto-sync running-config** is disabled when a processor card switchover occurs, the standby processor card uses the startup configuration.

In maintenance mode, all database synchronizing to the standby processor card is disabled even if **auto-sync running-config** is enabled.

Examples   The following example shows how to disable automatic synchronizing of the running configuration.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# no auto-sync running-config
```

Related Commands	Command	Description
	auto-sync startup-config	Selectively enables only automatic synchronizing of the startup configuration to the standby processor card.
	maintenance-mode	Disables all processor card redundancy synchronization.
	redundancy	Enters redundancy configuration mode.
	redundancy manual-sync	Causes an immediate one-time database update.
	show bootvar	Displays boot and other environmental variables.
	show redundancy summary	Displays processor card redundancy status and configuration information.

auto-sync startup-config

To selectively enable only automatic synchronizing of the startup configuration to the standby processor card, use the **auto-sync startup-config** command. To disable automatic synchronizing of the startup configuration, use the **no** form of this command.

auto-sync startup-config

no auto-sync startup-config

Syntax Description   This command has no other arguments or keywords.

Defaults   Enabled

Command Modes   Redundancy configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to enable or disable only automatic synchronizing of the startup configuration without affecting the following synchronization:

- Running configuration
- Dynamic database synchronizing

In maintenance mode, all database synchronizing to the standby processor card is disabled even if **auto-sync startup-config** is enabled.

Note   The system does not synchronize the startup configuration on the standby processor card if the startup configuration on the active processor card is corrupted.

Examples   The following example shows how to disable automatic synchronizing of the startup configuration.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)# no auto-sync startup-config
```

Related Commands

Command	Description
auto-sync running-config	Selectively enables only automatic synchronizing of the running configuration to the standby processor card.
maintenance-mode	Disables all processor card redundancy synchronization.
redundancy	Enters redundancy configuration mode.
redundancy manual-sync	Causes an immediate one-time database update.
show bootvar	Displays boot and other environmental variables.
show redundancy summary	Displays processor card redundancy status and configuration information.

clear redundancy

To clear redundancy history or counters, use the **clear redundancy** command.

clear redundancy {**history** | **counters**}

Syntax Description

history	Clears the redundancy event history log.
counters	Clears the redundancy internal operational counters.

Defaults   None

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to perform a one-time clear of the specified redundancy history or statistics database. This command may be useful for debugging or monitoring redundancy performance.

Examples   The following example shows how to clear the redundancy history log.

```
Switch# clear redundancy history
```

Related Commands

Command	Description
show redundancy counters	Displays redundancy software counter information.
show redundancy history	Displays redundancy software history information.

maintenance-mode

To disable all processor card redundancy synchronization, use the **maintenance-mode** redundancy command. To reenable redundancy synchronization, use the **no** form of this command.

    maintenance-mode

    no maintenance-mode

Syntax Description   This command has no other arguments or keywords.

Defaults   Disabled

Command Modes   Redundancy configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   In maintenance mode, the active processor card does not automatically synchronize information to the standby processor card. No standby processor card errors and alarms are reported to the active processor card. The standby processor card leaves the hot-standby mode, enters the negotiation state, and transitions to the cold-standby state.

When maintenance mode is disabled, the standby processor card reloads until it reaches the hot-standby state.

Maintenance mode is useful for processor card maintenance operations and system image troubleshooting.

Note   We do not recommend leaving the active and standby processor cards in maintenance mode for extended periods because any added configuration is lost unless the startup configuration on the active processor card is manually updated and manually synchronized with the standby processor card.

■ **maintenance-mode**

Examples   The following example shows how to enable maintenance mode redundancy.

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

Related Commands

Command	Description
redundancy	Enters redundancy configuration mode.
show redundancy summary	Displays processor card redundancy status and configuration information.

redundancy

To switch to redundancy configuration mode, use the **redundancy** command.

redundancy

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   Global configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to gain access to both processor card redundancy configuration commands and APS configuration commands.

Examples   The following example shows how to switch to redundancy configuration mode.

```
Switch# configure terminal
Switch(config)# redundancy
Switch(config-red)#
```

Related Commands

Command	Description
associate group	Associates wavepatch interfaces for APS splitter protection.
associate interface	Associates two interfaces for APS protection.
auto-sync running-config	Selectively enables only automatic synchronizing of the running configuration to the standby processor card.

Cisco ONS 15540 ESPx Command Reference Guide

Command	Description
auto-sync startup-config	Selectively enables only automatic synchronizing of the startup configuration to the standby processor card.
maintenance-mode	Enables or disables processor card redundancy synchronization.

redundancy manual-sync

To cause an immediate one-time database update of the specified database information, use the **redundancy manual-sync** command.

redundancy manual-sync {running-config | startup-config | both}

Syntax Description	running-config	Causes an immediate one-time update of the running configuration to the standby processor card.
	startup-config	Causes an immediate one-time update of the startup configuration to the standby processor card.
	both	Causes an immediate one-time update of the running configuration and the startup configuration to the standby processor card.

Defaults   None

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   This command is not usually required because automatic synchronization is enabled by default and, upon exiting global configuration mode, the running configuration is updated on the standby processor card. (Exit global configuration mode by entering **Ctrl-Z** or **end**.) The startup configuration is updated when the **copy** command is issued.

If auto-synchronizing is disabled, the **redundancy manual-sync** command updates the standby processor database information to be identical with the active processor card.

If the system is unable to complete the update, an error message is displayed.

This command is only allowed on the active processor card.

Examples   The following example shows how to make the active processor card send an update for both the running configuration and the startup configuration to the standby processor card.

```
Switch# redundancy manual-sync both
```

Related Commands

Command	Description
auto-sync running-config	Selectively enables only automatic synchronizing of the running configuration to the standby processor card.
auto-sync startup-config	Selectively enables only automatic synchronizing of the startup configuration to the standby processor card.
show redundancy summary	Displays processor card redundancy status and configuration information.

redundancy reload peer

To reload the standby processor card, use the **redundancy reload peer** command.

redundancy reload peer

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to reload the standby (or peer) processor card.

The active processor card is allowed to reload a standby processor card that is fully running the Cisco IOS software by using an NMI (non-maskable interrupt).

This command will not succeed on the active processor card if the standby processor card has not fully loaded its system IOS image and reached the hot-standby state.

This command cannot be entered on the standby processor card.

Examples   The following example shows how to reload the standby processor card.

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

Related Commands

Command	Description
maintenance-mode	Enables or disables processor card redundancy synchronization.
redundancy reload shelf	Reloads both processor cards in the shelf.
redundancy switch-activity	Manually switches activity from the active processor card to the standby processor card.
reload	Reloads the active processor card.
show redundancy summary	Displays processor card redundancy status and configuration information.

redundancy reload shelf

To reload both redundant processor cards, use the **redundancy reload shelf** command.

redundancy reload shelf

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   This command causes both processor cards to reload.

Examples   The following example shows how to reload the entire shelf.

```
Switch# redundancy reload shelf
Reload the entire shelf [confirm] y
Preparing to reload shelf
```

Related Commands

Command	Description
maintenance-mode	Enables or disables processor card redundancy synchronization.
redundancy reload peer	Reloads the standby processor card.
redundancy switch-activity	Manually switches activity from the active processor card to the standby processor card.

Command	Description
reload	Reloads the active processor card.
show redundancy summary	Displays processor card redundancy status and configuration information.

redundancy switch-activity

To manually switch activity from the active processor card to the standby processor card, use the **redundancy switch-activity** command.

redundancy switch-activity [**force**]

Syntax Description

force	Forces a switch of activity even when the standby processor card has not reached the hot-standby state, or if some other software condition is preventing a normal switchover from occurring.

Defaults   The active processor card switches over only if the standby processor card has reached hot-standby mode.

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   This command must be issued on the active processor card. It takes effect if the processor card is in a state to allow switchover; that is, the standby processor card is in the "Standby Hot" state and platform software is not temporarily disallowing the switchover.

Examples   The following example shows how to switch activity to the standby processor card.

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

01:40:35: %SYS-5-RELOAD: Reload requested
```

Related Commands

Command	Description
maintenance-mode	Enables or disables processor card redundancy synchronization.
redundancy reload peer	Reloads the standby processor card.
redundancy reload shelf	Reloads both processor cards in the shelf.
reload	Reloads the active processor card.
show redundancy summary	Displays processor card redundancy status and configuration information.

show redundancy capability

To display capabilities of the active and standby processor cards, use the **show redundancy capability** command.

> **show redundancy capability**

Syntax Description This command has no other arguments or keywords.

Defaults None

Command Modes Privileged EXEC

Command History This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines Use this command to display hardware and functional versions of the various components. If the capabilities do not match, the system is running in a degraded redundancy mode.

Examples The following example shows how to display capabilities for the active and standby processor cards. (See Table 6-1 for field descriptions.)

```
Switch# show redundancy capability

CPU capability support

 Active CPU  Sby CPU    Sby Compat      CPU capability description
 ----------  ----------  -----------  --------------------------------------
     96 MB      96 MB    OK           CPU DRAM size
     32 MB      32 MB    OK           CPU PMEM size
    512 KB     512 KB    OK           CPU NVRAM size
     16 MB      16 MB    OK           CPU Bootflash size
     3.5        3.5      OK           CPU hardware major.minor version
     1.20       1.18     OK           CPU functional major.minor version
```

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

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

Software sync client versions, listed as version range X-Y.
 X indicates the oldest peer version it can communicate with.
 Y indicates the current sync client version.
 Sync client counts: Active=2, Standby=2

 Active CPU   Sby CPU   Sby Compat  Cl ID  Redundancy Client description
 ---------- ---------- ----------- ----- -------------------------------------
 ver  1-1   ver  1-1   OK          17     CPU Redundancy
 ver  1-1   ver  1-1   OK          6      OIR Client


Backplane IDPROM comparison
 Backplane IDPROM field     Match Local CPU           Peer CPU
 ------------------------- ----- -------------------- --------------------
 idversion                  YES   1                    1
 magic                      YES   153                  153
 card_type                  YES   4102                 4102
 order_part_num_str         YES   N/A                  N/A
 description_str            YES   Manhattan_Backplane_PHASE_0
                                                       Manhattan_Backplane_PHASE_0
 board_part_num_str         YES   73-5655-03           73-5655-03
 board_revision_str         YES   02                   02
 serial_number_str          YES   TBC05031572          TBC05031572
 date_of_manufacture_str    YES   02/16/2001           02/16/2001
 deviation_numbers_str      YES   0                    0
 manufacturing_use          YES   0                    0
 rma_number_str             YES   0x00                 0x00
 rma_failure_code_str       YES   0x00                 0x00
 oem_str                    YES   Cisco_Systems        Cisco_Systems
 clei_str                   YES
 snmp_oid_substr            NO    0
 schematic_num_str          YES   92-4113-03           92-4113-03
 hardware_major_version     YES   3                    3
 hardware_minor_version     YES   0                    0
 engineering_use_str        YES   1                    1
 crc16                      OK    5913                 24184
 user_track_string          NO    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    0000164428fb0     0000164428fb0
cpu_number                    OK     1                 1
optical_backplane_type        YES    255               255
```

Table 6-1   show redundancy capability Field Descriptions

Field	Description
Active CPU	Shows the following information for the active processor card:
	• processor DRAM size—the size of dynamic random access memory
	• processor PMEM size—the amount of dynamic RAM reserved for packet I/O usage
	• processor NVRAM size—the size of nonvolatile RAM
	• processor Bootflash size—the size of bootflash memory
	• processor hardware major.minor version—the processor card hardware version
	• processor functional major.minor version—the processor card functional version
Sby CPU	Shows information for the standby processor card. See the "Active CPU" description above.
Sby Compat	Indicates whether the standby processor card is compatible with the active processor card.
CPU capability description	Shows the capability descriptions for the active and standby processor cards. See the "Active CPU" description above.
Linecard driver major.minor versions	Shows the number of line card drivers.
Drv ID	Shows the driver ID.
Driver description	Shows the driver description.
Software sync client versions	Shows the redundancy client version in the range X-Y, where:
	• X indicates the oldest peer version it can communicate with.
	• Y indicates the current sync client version.
	Also shows the sync client counts.
Cl ID	Shows the client ID.
Redundancy Client description	Shows the redundancy client descriptions.

Related Commands

Command	Description
redundancy	Switches to redundancy configuration mode.
redundancy manual-sync	Causes an immediate one-time update of the specified database.
redundancy reload peer	Reloads the redundant peer processor card.
redundancy reload shelf	Reloads both redundant processor cards in the shelf.

Command	Description
redundancy switch-activity	Manually switches activity from the active processor card to the current standby processor card.
show redundancy summary	Displays processor card redundancy status and configuration information.

show redundancy clients

To display a list of internal redundancy clients, use the **show redundancy clients** command.

show redundancy clients

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   EXEC and privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to display information about the software subsystems that are clients of the platform-independent RF (Redundancy Facility) subsystem. Subsystems that need to synchronize information from the active processor card to the standby processor card (or vice versa) are registered as clients of the RF.

This client information can be used to debug redundancy software.

Examples   The following example shows how to display a list of internal redundancy clients. (See Table 6-2 for field descriptions.)

```
Switch# show redundancy clients
 clientID = 0      clientSeq = 0        RF_INTERNAL_MSG
 clientID = 6      clientSeq = 16       OIR Client
 clientID = 17     clientSeq = 40       CPU Redundancy
 clientID = 19     clientSeq = 9999     RF_LAST_CLIENT
```

Table 6-2   show redundancy clients Field Descriptions

Field	Description
clientID	Shows the ID of the redundant client.
clientSeq	Shows the client notification sequence number.
	Client sequence numbers determine the order in which a client is notified of RF events, relative to other clients. There are cases where one client must be notified before another. This should be noted when the sequence number is defined. The lower sequence numbers are notified first.
RF_INTERNAL_MSG	Shows the RF first client, which is part of the RF subsystem and is necessary for its operation.
OIR Client	Shows the OIR (online insertion and removal) client, which updates the standby processor card when line cards are inserted and removed.
CPU Redundancy	Shows the processor card redundancy client, which sends running or startup configuration changes to the standby processor card. This client also reports hardware/software compatibility and version numbers between the processor cards. It also ensures that processor card arbitration changes and peer processor card communication losses are reported to the RF and to other subsystems.
RF_LAST_CLIENT	Shows the RF last client, which is part of the RF subsystem and is necessary for its operation.

Related Commands

Command	Description
redundancy	Switches to redundancy configuration mode.
redundancy manual-sync	Causes an immediate one-time update of the specified database.
redundancy reload peer	Reloads the redundant peer processor card.
redundancy reload shelf	Reloads both redundant processor cards in the shelf.
redundancy switch-activity	Manually switches activity from the active processor card to the current standby processor card.
show redundancy summary	Displays processor card redundancy status and configuration information.

show redundancy counters

To display internal redundancy software counters, use the **show redundancy counters** command.

show redundancy counters

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to display internal redundancy software counter information, which can be used to debug redundancy software.

Examples   The following example shows how to display internal redundancy software counter information. (See Table 6-3 for field descriptions.)

```
Switch# show redundancy counters
Redundancy Facility OMs
              comm link up = 1
        comm link down down = 0

          invalid client tx = 0
          null tx by client = 0
                tx failures = 0
      tx msg length invalid = 0

        client not rxing msgs = 0
  rx peer msg routing errors = 0
            null peer msg rx = 0
```

```
      errored peer msg rx = 0

                buffers tx = 656
     tx buffers unavailable = 0
                buffers rx = 1302
      buffer release errors = 0

 duplicate client registers = 0
   failed to register client = 0
       Invalid client syncs = 0
```

Table 6-3   *show redundancy counters Field Descriptions*

Field	Description
comm link up	Shows how many communications links are up.
comm link down down	Shows how many communications links are down.
invalid client tx	Shows the number of invalid client transmissions.
null tx by client	Shows the number of null transmissions by the client.
tx failures	Shows the number of transmission failures.
tx msg length invalid	Shows the number of transmission messages with invalid lengths.
client not rxing msgs	Shows that the client is not receiving event messages.
rx peer msg routing errors	Shows errors occurring in the RF application. This usually indicates a software problem.
null peer msg rx	Shows that the interprocess communication (IPC) has sent an empty message to the RF application. This usually indicates a software problem.
errored peer msg rx	Shows an IPC error when an RF message was received. This usually indicates a software problem.
buffers tx	Shows the number of internal buffers acquired for sending RF messages.
tx buffers unavailable	Shows the number of times internal buffers for sending RF messages were not available due to the high volume of messages being sent. This usually indicates a software problem.
buffers rx	Shows the number of buffers released back to the internal buffer pool.
buffer release errors	Shows errors in releasing internal buffers.
duplicate client registers	Shows that an application has been registered with the RF more than once. This usually indicates a software problem.
failed to register client	Shows that the system was unable to register an RF client application due to low memory or due to a software problem.
Invalid client syncs	Shows an internal software problem in the RF.

Related Commands

Command	Description
redundancy	Switches to redundancy configuration mode.
redundancy manual-sync	Causes an immediate one-time update of the specified database.
redundancy reload peer	Reloads the standby processor card.
redundancy reload shelf	Reloads both redundant processor cards in the shelf.

Command	Description
redundancy switch-activity	Manually switches activity from the active processor card to the current standby processor card.
show redundancy summary	Displays processor card redundancy status and configuration information.

show redundancy history

To display internal redundancy software history, use the **show redundancy history** command.

show redundancy history

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

EXEC and privileged EXEC

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to display the internal redundancy software history log, which can be used to debug redundancy software.

Examples

The following example shows how to display the internal redundancy software history log, which can be useful for debugging redundancy software. (See Table 6-4 for field descriptions.)

```
Switch# show redundancy history
Redundancy Facility Event Log:
00:00:00 client added: RF_INTERNAL_MSG(0) seq=0
00:00:00 client added: RF_LAST_CLIENT(19) seq=9999
00:00:16 client added: CPU Redundancy(17) seq=40
00:00:16 *my state = INITIALIZATION(2) *peer state = DISABLED(1)
00:00:16 RF_PROG_INITIALIZATION(0) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:16 RF_PROG_INITIALIZATION(0) CPU Redundancy(17) op=0 rc=11
00:00:16 RF_PROG_INITIALIZATION(0) RF_LAST_CLIENT(19) op=0 rc=11
00:00:16 *my state = NEGOTIATION(3) peer state = DISABLED(1)
00:00:16 RF_STATUS_PEER_PRESENCE(12) op=0
00:00:16 RF_EVENT_GO_ACTIVE(28) op=0
00:00:16 *my state = ACTIVE-FAST(9) peer state = DISABLED(1)
```

```
00:00:16 RF_STATUS_SPLIT_ENABLE(15) CPU Redundancy(17) op=0
00:00:16 RF_PROG_ACTIVE_FAST(6) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:16 RF_PROG_ACTIVE_FAST(6) CPU Redundancy(17) op=0 rc=11
00:00:16 RF_PROG_ACTIVE_FAST(6) RF_LAST_CLIENT(19) op=0 rc=11
00:00:16 *my state = ACTIVE-DRAIN(10) peer state = DISABLED(1)
00:00:16 RF_PROG_ACTIVE_DRAIN(7) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:16 RF_PROG_ACTIVE_DRAIN(7) CPU Redundancy(17) op=0 rc=11
00:00:16 RF_PROG_ACTIVE_DRAIN(7) RF_LAST_CLIENT(19) op=0 rc=11
00:00:16 *my state = ACTIVE_PRECONFIG(11) peer state = DISABLED(1)
00:00:16 RF_PROG_ACTIVE_PRECONFIG(8) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:16 RF_PROG_ACTIVE_PRECONFIG(8) CPU Redundancy(17) op=0 rc=11
00:00:16 RF_PROG_ACTIVE_PRECONFIG(8) RF_LAST_CLIENT(19) op=0 rc=11
00:00:16 *my state = ACTIVE_POSTCONFIG(12) peer state = DISABLED(1)
00:00:16 RF_PROG_ACTIVE_POSTCONFIG(9) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:16 RF_PROG_ACTIVE_POSTCONFIG(9) CPU Redundancy(17) op=0 rc=11
00:00:16 RF_PROG_ACTIVE_POSTCONFIG(9) RF_LAST_CLIENT(19) op=0 rc=11
00:00:16 *my state = ACTIVE(13) peer state = DISABLED(1)
00:00:16 RF_PROG_ACTIVE(10) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:16 RF_PROG_ACTIVE(10) CPU Redundancy(17) op=0 rc=11
00:00:16 RF_PROG_ACTIVE(10) RF_LAST_CLIENT(19) op=0 rc=11
00:00:16 client added: OIR Client(6) seq=16
00:00:19 RF_STATUS_PEER_PRESENCE(12) op=0
00:00:36 Configuration parsing complete
00:00:36 System initialization complete
```

Table 6-4   show redundancy history Field Descriptions

Field	Description
client added	Shows the RF subsystem client added.
*my state = INITIALIZATION	Shows that the processor card has been initialized.
*peer state = DISABLED	Shows that the peer (or standby) processor card is disabled.
Configuration parsing complete	Shows that the configuration has been read either from NVRAM or, on a switchover, from the stored running-config file.
System initialization complete	Shows that the system initialization is complete.

Related Commands	Command	Description
	clear redundancy	Clears the redundancy history buffer in processor memory.
	redundancy	Switches to redundancy configuration mode.
	redundancy manual-sync	Causes an immediate one-time update of the specified database.
	redundancy reload peer	Reloads the standby processor card.
	redundancy reload shelf	Reloads both redundant processor cards in the shelf.
	redundancy switch-activity	Manually switches activity from the active processor card to the current standby processor card.
	show redundancy summary	Displays processor card redundancy status and configuration information.

show redundancy running-config-file

To display the running configuration on the standby processor card, use the **show redundancy running-config-file** command.

show redundancy running-config-file

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   EXEC and privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   This command is only available on the standby processor card. It shows the stored running-config file that has been synchronized from the active processor card, which will be applied as the system configuration during the next standby to active transition.

If auto-synchronization is disabled for the running-config-file on the active processor card, or if the IPC (interprocessor communications) is down, this command displays the message `running-config-file is not currently valid` and does not show the running-configuration file.

Note   While the standby processor card remains in the hot-standby state, the running configuration, as shown by the **show running-config** command, is not expected to match the synchronized running-config file. Instead, it contains mostly default configuration values.

Examples   The following example displays the running-config file on the standby processor card. See Table 6-5 for field descriptions.

```
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
!
hostname Switch
!
boot system flash bootflash:ons15540-i-mz
boot bootldr slot0:ons15540-i-mz

<Information deleted>
```

Table 6-5   show redundancy running-config-file Field Descriptions

Field	Description
version	Shows the software version.
no service pad	Shows service pad configuration. In the output example, "no" indicates that incoming and outgoing packet assembler/disassembler (PAD) connections are not accepted.
service timestamps	Shows that logging appears with timestamps.
no service password-encryption	Shows that password encryption has been disabled.
hostname	Shows the system name.
boot system flash	Shows the boot system flash version.
boot bootldr	Shows the bootldr version.

Related Commands

Command	Description
redundancy	Switches to redundancy configuration mode.
redundancy manual-sync	Causes an immediate one-time update of the specified database.
redundancy reload peer	Reloads the redundant peer processor card.
redundancy reload shelf	Reloads both redundant processor cards in the shelf.
redundancy switch-activity	Manually switches activity from the active processor card to the current standby processor card.
show redundancy summary	Displays processor card redundancy status and configuration information.

show redundancy states

To display internal redundancy software state information, use the **show redundancy states** command.

show redundancy states

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   EXEC and privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to display internal redundancy software state information, which may be used to debug redundancy software.

Examples   The following example shows how to display internal redundancy software state information. (See Table 6-6 for field descriptions.)

```
Switch> show redundancy states
      my state = 13 -ACTIVE
    peer state = 8  -STANDBY HOT
          Mode = Duplex
       Unit ID = 6

    Split Mode = Disabled
  Manual Swact = Enabled
Communications = Up

  client count = 5
client_notification_TMR = 30000 milliseconds
        keep_alive TMR = 5000 milliseconds
```

```
      keep_alive count = 1
 keep_alive threshold = 10
        RF debug mask = 0x0
```

Table 6-6   show redundancy states Field Descriptions

Field	Description
my state	Shows the state of the active processor card.
peer state	Shows the state of the peer (or standby) processor card.
Mode	Shows either simplex (single processor card) or duplex (two processor cards) mode.
Unit	Shows either primary (or active) processor card or peer (or standby) processor card.
Unit ID	Shows the unit ID of the processor card.
Split Mode	Indicates whether split mode is enabled or disabled.
Manual Swact	Indicates whether manual switchovers have been enabled without the force option.
Reason	Shows why manual switchovers have been disabled. Valid reasons are: • Simplex mode • Invalid peer state • Split mode • Progression in progress • Unidentified platform-specific reason
Communications	Indicates whether communications are up or down between the two processor cards.
Reason	Shows why communications are down, either because the system is in simplex mode or due to a failure.
client count	Shows the number of redundancy subsystems that are registered as RF clients.
client_notification_TMR	Shows, in milliseconds, the time that an internal RF timer has for notifying RF client subsystems.
keep_alive TMR	Shows, in milliseconds, the time interval the RF manager has for sending keep-alive messages to its peer on the standby processor card.
keep_alive count	Shows the number of keep-alive messages sent without receiving a response from the standby processor card.
keep_alive threshold	Shows the threshold for declaring that interprocessor communications are down when keep-alive messages have been enabled (which is the default).
RF debug mask	Shows an internal mask used by the RF to keep track of which debug modes are on.

Related Commands

Command	Description
redundancy	Switches to redundancy configuration mode.
redundancy manual-sync	Causes an immediate one-time update of the specified database.
redundancy reload peer	Reloads the redundant standby processor card.
redundancy reload shelf	Reloads both redundant processor cards in the shelf.
redundancy switch-activity	Manually switches activity from the active processor card to the current standby processor card.
show redundancy summary	Displays processor card redundancy status and configuration information.

show redundancy summary

To display a summary of active and standby processor card redundancy information, use the **show redundancy summary** command.

> **show redundancy summary**

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   EXEC and privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.1(18)SV	This command was integrated in this release anda dded the **summary** keyword.

S-Release	Modification
12.2(22)S	This command was integrated in this relase and added the **summary** keyword.

Usage Guidelines   Use this command to display a summary of redundancy-related information, including active and standby slots, uptimes, images, and current alarms. This information is useful for troubleshooting processor card redundancy problems.

Examples   The following example shows how to display a summary of redundancy-related information for the system. (See Table 6-7 for field descriptions.)

```
Switch# show redundancy summary


Redundant system information
----------------------------
Available Uptime:            12 minutes
Time since last switchover:  6 minutes
Switchover Count:            2
```

```
Inter-CPU Communication State:UP
Last Restart Reason:          Switch over
Reported Switchover Reason:   User initiated
Software state at switchover: STANDBY HOT

Last Running Config sync:     2 minutes
Running Config sync status:   In Sync
Last Startup Config sync:     2 minutes
Startup Config sync status:   In Sync

This CPU is the Active CPU.
------------------------------
Slot:                         6
Time since CPU Initialized:   8 minutes
Image Version:                ONS-15540 Software (ONS15540-I-M), Released Version
Image File:                   slot0:ons15540-i-mz
Software Redundancy State:    ACTIVE
Hardware State:               ACTIVE
Hardware Severity:            0

Peer CPU is the Standby CPU.
------------------------------
Slot:                         7
Time since CPU Initialized:   2 minutes
Image Version:                ONS-15540 Software (ONS15540-I-M), Released Version
Image File (on sby-CPU):      slot0:ons15540-i-mz
Software Redundancy State:    STANDBY HOT
Hardware State:               STANDBY
Hardware Severity:            0
Privilege Mode:               Disabled
```

Table 6-7   show redundancy summary Field Descriptions

Field	Description
Available Uptime	Shows the elapsed time since the system began providing uninterrupted operation, including the time when either processor card is active.
Time since last switchover	Shows the amount of time since the last switchover.
Switchover Count	Shows the number of times switchover has occurred during the Available Uptime.
Inter-CPU Communication State	Shows the status of IPC (interprocess communications).
Last Restart Reason	Shows the reason for the last restart. Valid reasons include normal boot and switchover.
Last Switchover Reason	Shows the reason for the last switchover when the Last Restart Reason field shows "Switch over." Valid reasons are: • Not known • User initiated • User forced • User forced (reload) • Active unit failed • Active unit removed

Table 6-7   show redundancy summary Field Descriptions (continued)

Field	Description
Software state at switchover	Shows the software redundancy state of the processor at the time of the last switchover.
Last Running Config sync	Shows the amount of time since the processor card was synchronized with the last running configuration.
Running Config sync status	Indicates whether the processor card is in sync with the running configuration.
Last Startup Config sync	Shows the amount of time since the processor card was synchronized with the last startup configuration.
Startup Config sync status	Indicates whether the processor card is in sync with the startup configuration.
Slot	Shows the slot number on the active or standby system.
Time since CPU Initialized	Shows the amount of time since the active or standby processor card was last initialized.
Image	Shows the active or standby processor card system image and version.
Software Redundancy State	Indicates whether software redundancy is enable for the active and standby processor card.
Hardware State	Shows the hardware state of the active or standby processor card.
Hardware Severity	Shows the severity of hardware faults. Valid values are: • 0 = good processor card hardware (no hardware faults) • 1 = processor card hardware fault that does not affect traffic • 2 = fault that partially affects traffic • 3 = fault that may affect all user data traffic
Privilege Mode	Shows whether privileged EXEC mode is accessible on the standby processor card CLI.

Related Commands

Command	Description
redundancy	Switches to redundancy configuration mode.
redundancy manual-sync	Causes an immediate one-time update of the specified database.
redundancy reload peer	Reloads the redundant peer processor card.
redundancy reload shelf	Reloads both redundant processor cards in the shelf.
redundancy switch-activity	Manually switches activity from the active processor card to the current standby processor card.
show redundancy capability	Displays processor card redundancy capability information.
standby privileged-mode enable	Enables or disables access to privileged EXEC mode on the standby processor card CLI.

standby privileged-mode enable

To allow users to access privileged EXEC command mode on the standby processor card, use the **standby privileged-mode enable** command. To disallow access to privileged EXEC command mode on the standby processor card, use the **no** form of this command.

> **standby privileged-mode enable**

> **no standby privileged-mode enable**

Syntax Description   This command has no other arguments or keywords.

Defaults   Enable mode is disabled on the standby processor card.

Command Modes   Redundancy configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   The **enable** command allows you to access privileged EXEC commands. On the active processor card, you can configure authentications to prevent unauthorized access in addition to the enable and secret passwords. No such authentications are available on the standby processor card. The **standby privileged-mode enable** command provides extra security for your system by allowing you to control access to the **enable** command on the standby processor card CLI.

> **Note**   You can only enter the **standby privileged-mode enable** command on the active processor card CLI.

Examples   The following example shows how to allow access to privileged EXEC command mode on the standby processor card.

```
Switch# configure terminal
```

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

	Command	Description
Related Commands	**redundancy**	Enters redundancy configuration mode.
	show redundancy summary	Displays processor card redundancy status and configuration information.

7

SNMP Commands

This chapter contains the Cisco ONS 15540 ESPx-specific SNMP commands. For the complete list of SNMP commands supported on the Cisco ONS 15540 ESPx, and their descriptions, refer to *Cisco IOS Configuration Fundamentals Command Reference* publication.

snmp-server enable traps aps

To enable SNMP trap notifications for APS activity, use the **snmp-server enable traps aps** command. To disable this feature, use the **no** form of the command.

snmp-server enable traps aps

no snmp-server enable traps aps

Syntax Description   This command has no other arguments or keywords.

Defaults   Disabled

Command Modes   Global configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to enable the SNMP trap notifications defined in the APS MIB (CISCO-APS-MIB).

The **snmp-server enable traps aps** command is used in conjunction with the **traceroute** command. For a host to receive SNMP trap notifications for APS activity, the **snmp-server enable traps aps** command and the **traceroute** command for that host must be enabled.

Examples   The following example shows how to enable SNMP trap notifications for APS activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps aps
```

Related Commands	Command	Description
	associate interface	Specifies interfaces to be associated and enters APS configuration mode.
	show aps	Displays APS configuration information and status.
	show running-config	Displays the configuration information currently running on the system.
	traceroute	Specifies the recipient for SNMP notification messages.

snmp-server enable traps cdl

To enable SNMP trap notifications defined in CISCO-CDL-MIB, use the **snmp-server enable traps cdl** command. To disable this feature, use the **no** form of the command.

> **snmp-server enable traps cdl** {**all** | **terminating-interfaces**} [**soak-interval** *set-soak-interval clear-soak-interval*]

> **no snmp-server enable traps cdl** {**all** | **terminating-interfaces**} [**soak-interval** *set-soak-interval clear-soak-interval*]

Syntax Description

all	Enables trap notifications on all in-band message channel capable interfaces.
terminating-interfaces	Enables trap notifications only on terminating interfaces for in-band message channel traffic.
soak-interval	Sets interval after which trap notifications are sent.
set-soak-interval	Indicates time interval in milliseconds before sending defect indication trap notifications when a defect is set. The range is 100 to 60,000.
clear-soak-interval	Indicates time interval in milliseconds before sending defect indication trap notifications when a defect is cleared. The range is 100 to 60,000.

Defaults

Disabled

Set interval: 2500 milliseconds

Clear interval: 10,000 milliseconds

Command Modes

Global configuration

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV2	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to enable the SNMP trap notifications defined in the in-band message channel MIB (CISCO-CDL-MIB). SNMP trap notifications are sent when an in-band message channel connection is created, modified, or deleted.

The soak interval prevents the system from being flooded with set and clear notifications for defect indications. The default values for the soak interval are adequate for most network topologies.

The **snmp-server enable traps cdl** command is used in conjunction with the **snmp-server host** command. For a host to receive SNMP trap notifications for patch connection activity, the **snmp-server enable traps cdl** command and the **snmp-server host** command for that host must be enabled.

Examples   The following example shows how to enable SNMP trap notifications for patch connection activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps cdl all
```

Related Commands

Command	Description
show running-config	Displays the configuration information currently running on the system.
snmp-server host	Specifies the recipient for SNMP notification messages.

snmp-server enable traps patch

To enable SNMP trap notifications for patch connection activity, use the **snmp-server enable traps patch** command. To disable this feature, use the **no** form of the command.

snmp-server enable traps patch

no snmp-server enable traps patch

Syntax Description   This command has no other arguments or keywords.

Defaults   Disabled

Command Modes   Global configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to enable the SNMP trap notifications defined in the OSCP MIB (CISCO-OPTICAL-PATCH-MIB). SNMP trap notifications are sent when a patch connection is created, modified, or deleted.

The **snmp-server enable traps patch** command is used in conjunction with the **traceroute** command. For a host to receive SNMP trap notifications for patch connection activity, the **snmp-server enable traps patch** command and the **traceroute** command for that host must be enabled.

Examples   The following example shows how to enable SNMP trap notifications for patch connection activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps patch
```

Related Commands

Command	Description
patch	Configures patch connections.
show patch	Displays patch connection information.
show running-config	Displays the configuration information currently running on the system.
traceroute	Specifies the recipient for SNMP notification messages.

snmp-server enable traps cdl

To enable SNMP trap notifications defined in CISCO-CDL-MIB, use the **snmp-server enable traps cdl** command. To disable this feature, use the **no** form of the command.

> **snmp-server enable traps cdl** {**all** | **terminating-interfaces**} [**soak-interval** *set-soak-interval clear-soak-interval*]

> **no snmp-server enable traps cdl** {**all** | **terminating-interfaces**} [**soak-interval** *set-soak-interval clear-soak-interval*]

Syntax Description

all	Enables trap notifications on all in-band message channel capable interfaces.
terminating-interfaces	Enables trap notifications only on terminating interfaces for in-band message channel traffic.
soak-interval	Sets interval after which trap notifications are sent.
set-soak-interval	Specifies time interval in milliseconds before sending defect indication trap notifications when a defect is set. The range is 100 to 60,000.
clear-soak-interval	Specifies time interval in milliseconds before sending defect indication trap notifications when a defect is cleared. The range is 100 to 60,000.

Defaults

Disabled

Set interval: 2500 milliseconds

Clear interval: 10,000 milliseconds

Command Modes

Global configuration

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV2	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to enable the SNMP trap notifications defined in the in-band message channel MIB (CISCO-CDL-MIB). SNMP trap notifications are sent when an in-band message channel connection is created, modified, or deleted.

The soak interval prevents the system from being flooded with set and clear notifications for defect indications. The default values for the soak interval are adequate for most network topologies.

The **snmp-server enable traps cdl** command is used in conjunction with the **snmp-server host** command. For a host to receive SNMP trap notifications for patch connection activity, the **snmp-server enable traps cdl** command and the **snmp-server host** command for that host must be enabled.

Examples   The following example shows how to enable SNMP trap notifications for patch connection activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps cdl all
```

Related Commands

Command	Description
show running-config	Displays the configuration information currently running on the system.
snmp-server host	Specifies the recipient for SNMP notification messages.

snmp-server enable traps oscp

To enable SNMP trap notifications for OSCP activity, use the **snmp-server enable traps oscp** command. To disable this feature, use the **no** form of the command.

snmp-server enable traps oscp

no snmp-server enable traps oscp

Syntax Description   This command has no other arguments or keywords.

Defaults   Disabled

Command Modes   Global configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to enable the SNMP trap notifications defined in the OSCP MIB (CISCO-OSCP-MIB).

The **snmp-server enable traps oscp** command is used in conjunction with the **traceroute** command. For a host to receive SNMP trap notifications for OSCP activity, the **snmp-server enable traps oscp** command and the **traceroute** command for that host must be enabled.

Examples   The following example shows how to enable SNMP trap notifications for OSCP activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps oscp
```

Related Commands

Command	Description
show oscp info	Displays OSCP configuration information.
show oscp neighbor	Displays OSCP neighbor information.
show running-config	Displays the configuration information currently running on the system.
traceroute	Specifies the recipient for SNMP notification messages.

snmp-server enable traps rf

To enable SNMP trap notification for processor card redundancy activity, use the **snmp-server enable traps rf** command. To disable this feature, use the **no** form of the command.

snmp-server enable traps rf

no snmp-server enable traps rf

Syntax Description   This command has no other arguments or keywords.

Defaults   Disabled

Command Modes   Global configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to enable the SNMP trap notifications defined in the Redundancy Facility MIB (CISCO-RF-MIB).

The **snmp-server enable traps patch** command is used in conjunction with the **traceroute** command. For a host to receive SNMP trap notifications for patch connection activity, the **snmp-server enable traps patch** command and the **traceroute** command for that host must be enabled.

Examples   The following example shows how to enable SNMP trap notifications for processor card redundancy activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps rf
```

Related Commands	Command	Description
	redundancy	Enters redundancy configuration mode.
	show redundancy summary	Displays redundancy configuration information and status.
	show running-config	Displays the configuration information currently running on the system.
	traceroute	Specifies the recipient for SNMP notification messages.

snmp-server enable traps threshold min-severity

To enable SNMP trap notifications for alarm thresholds, use the **snmp-server enable traps threshold min-severity** command. To disable this feature, use the **no** form of this command.

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

no snmp-server enable traps threshold min-severity

Syntax Description	**degrade** Specifies signal degrade as the minimum severity for SNMP trap notifications.
	failure Specifies signal failure as the minimum severity for SNMP trap notifications.

Defaults   Disabled

Command Modes   Global configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to enable the SNMP trap notifications defined in the alarm threshold MIB (CISCO-IF-THRESHOLD-MIB).

The **snmp-server enable traps threshold min-severity** command is used in conjunction with the **traceroute** command. For a host to receive SNMP trap notifications for alarm threshold activity, the **snmp-server enable traps threshold min-severity** command and the **traceroute** command for that host must be enabled.

Examples   The following example shows how to enable SNMP trap notifications for alarm threshold activity and set the minimum severity to failure.

```
Switch# configure terminal
```

```
Switch(config)# snmp-server enable traps threshold min-severity failure
```

	Command	Description
Related Commands	show running-config	Displays the configuration information currently running on the system.
	show threshold-list	Displays the contents of a threshold list.
	traceroute	Specifies the recipient for SNMP notification messages.
	threshold-list	Groups a set of thresholds with a name. Switches from configuration mode to threshold-list configuration mode.

snmp-server enable traps topology

To enable SNMP trap notifications for the network topology activity, use the **snmp-server enable traps topology** command. To disable this feature, use the **no** form of the command.

> **snmp-server enable traps topology** [**throttle-interval** *seconds*]

> **no snmp-server enable traps topology** [**throttle-interval** *seconds*]

Syntax Description

throttle-interval *seconds*	Specifies the number of seconds for the throttle timer interval. Valid values are 5 through 3600 seconds. If this keyword is omitted, the command defaults to 60 seconds at bootup time, or to the previous value configured.

Defaults   Disabled

Command Modes   Global configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to enable the SNMP trap notifications defined in the physical topology MIB (PTOPO-MIB).

The network topology trap throttle timer prevents the system from flooding the network with messages. We recommend a 60-second interval value.

The **snmp-server enable traps topology** command is used in conjunction with the **traceroute** command. For a host to receive SNMP trap notifications for physical topology activity, the **snmp-server enable traps topology** command and the **traceroute** command for that host must be enabled.

Examples   The following example shows how to enable SNMP trap notifications for network topology activity and set the throttle timer interval to 30 seconds.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps topology throttle-interval 30
```

The following example shows how to enable SNMP trap notifications for network topology activity and set the throttle timer interval to the default value.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps topology
```

	Command	Description
Related Commands	show running-config	Displays the configuration information currently running on the system.
	traceroute	Specifies the recipient for SNMP notification messages.
	show topology	Displays global physical topology configuration.
	topology neighbor cdp	Enables CDP on the interface.

snmp-server host

To specify the recipient for SNMP notification messages, use the **snmp-server host** command. To remove the specified host, use the **no** form of the command.

snmp-server host *host-addr* [**traps** | **informs**] [**version** [**1** | **2c** | **3** {**auth** | **noauth**}]] *community-string* [**udp-port** *port*] [*notification-type*]

no snmp-server host *host-addr* {**traps** | **informs**}

Syntax Description

host-addr	Specifies the name or IP address of the targeted recipient host.
traps	Sends SNMP trap notifications to this host. This is the default. (Optional)
informs	Sends SNMP inform notifications to this host. (Optional)
version	Specifies the version of the SNMP used to send the traps. (Optional)
	Version 3 is the most secure model, as it allows packet encryption with the **priv** keyword. If you use the **version** keyword, one of the following must be specified:
	• **1** —SNMPv1. This option is not available with informs.
	• **2c** —SNMPv2C.
	• **3** —SNMPv3. The following three optional keywords can follow the version 3 keyword:
	– **auth**—Enables MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) packet authentication
	– **noauth**—Gives the noAuthNoPriv security level. This is the default if no keyword is specified.
community-string	Specifies the password-like community string sent with the notification operation. Though you can set this string using the **snmp-server host** command by itself, we recommend you define this string using the **snmp-server community** command prior to using the **snmp-server host** command.

udp-port *port*	Specifies the UDP port of the host to use. The range is 0 to 65535. The default is 162. (Optional)
notification-type	Specifies the type of notification to be sent to the host. (Optional)
	If no type is specified, all notifications are sent. The notification type can be one or more of the following keywords:
	• **alarms**—Sends alarm state change notifications (CISCO-ENTITY-ALARM-MIB).
	• **aps**—Sends APS MIB (CISCO-APS-MIB) modification notifications.
	• **bgp**—Sends BGP (Border Gateway Protocol) state change notifications.
	• **cdl**—Sends in-band message channel MIB (CISCO-CDL-MIB) modification notifications.
	• **config**—Sends configuration notifications.
	• **entity**—Sends entity MIB (ENTITY-MIB) modification notifications.
	• **fru-ctrl**—Sends entity FRU (field replaceable unit) control MIB (CISCO-ENTITY-FRU-CONTROL-MIB) modification notifications.
	• **oscp**—Sends OSCP MIB (CISCO-OSCP-MIB) modification notifications.
	• **patch**—Sends optical patch MIB (CISCO-OPTICIAL-PATCH-MIB) modification notifications.
	• **rf**—Sends redundancy facility MIB (CISCO-RF-MIB) modification notifications.
	• **snmp**—Sends SNMP notifications (as defined in RFC 1157).
	• **syslog**—Sends error message notifications (CISCO-SYSLOG-MIB). Specify the level of messages to be sent with the logging history level command.
	• **threshold**—Sends interface alarm threshold MIB (CISCO-IF-THRESHOLD-MIB) modification notifications.
	• **topology**—Sends physical topology MIB (PTOPO-MIB) modification notifications.
	• **tty**—Sends Cisco enterprise-specific notifications when a TCP connection closes.

Defaults   This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs are sent to this host.

If no **version** keyword is present, the default is version 1.

Command Modes   Global configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request is held in memory until a response is received or the request times out. Also, traps are sent only once, while an inform might be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the system to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host.

To enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host** command to enable informs for a host and then enter another **snmp-server host** command to enable informs for the same host, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

Some notification types cannot be controlled with the **snmp-server enabl**e command. Certain notification types are always enabled. Other notification types are enabled by a different command. For example, the linkUpDown notifications are controlled by the **snmp trap link-status** command. These notification types do not require an **snmp-server enable** command.

Examples   The following example shows how to enable SNMP trap notifications for APS activity.

```
Switch# configure terminal
Switch(config)# snmp-server host node1 traps
```

Related Commands	Command	Description
	show running-config	Displays the configuration information currently running on the system.
	show snmp	Displays the status of SNMP communications.
	snmp-server enable traps aps	Enables SNMP trap notification for APS activity.
	snmp-server enable traps oscp	Enables SNMP trap notifications for OSCP activity.
	snmp-server enable traps patch	Enables SNMP trap notifications for patch connection activity.
	snmp-server enable traps rf	Enables SNMP trap notifications for redundancy facility activity.
	snmp-server enable traps threshold min-severity	Enables SNMP trap notifications for alarm threshold activity.
	snmp-server enable traps topology	Enables SNMP trap notifications for physical topology activity.

System Management Commands

Use the following commands to manage your Cisco ONS 15540 ESPx.

clear facility-alarm

To clear the external indications for the facility alarms, use the **clear facility-alarm** command.

clear facility-alarm [**critical** | **major** | **minor**]

Syntax Description

critical	Specifies that all external critical alarm indications be cleared.
major	Specifies that all external major alarm indications be cleared.
minor	Specifies that all external minor alarm indications be cleared.

Defaults   Clears all external alarm indications and LEDs.

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to perform a one-time clear of the specified LEDS and external audible and visual alarm relays.

The facility alarm conditions and alarm threshold error conditions are still posted in the processor memory and can be seen by using the **show facility-alarm status** command. You can clear the alarm threshold error conditions in memory by disabling protocol monitoring using the **no monitor enable** command. Online removal of a component or disabling an interface with the **show performance** command also clears an alarm from processor memory.

Examples   The following examples shows how to clear critical external facility alarm indications.

```
Switch# clear facility-alarm critical
```

Related Commands	Command	Description
	monitor enable	Enables signal monitoring for certain protocol encapsulations.
	show facility-alarm status	Shows the facility alarm status information.
	show performance	Disables an interface.

environment-monitor shutdown fan

To enable fan failure shutdown, use the **environment-monitor shutdown fan** command. To disable fan failure shutdown, use the **no** form of the command.

environment-monitor shutdown fan

no environment-monitor shutdown fan

Syntax Description   This command has no other arguments or keywords.

Defaults   Disabled

Command Modes   Global configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(12c)EV3	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   If a single fan fails on the Cisco ONS 15540 ESPx, a minor alarm is reported to the processor card. However, the chassis will never reach critical high temperature when only one fan fails.

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

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

To prevent damage to the cards and modules in the shelf when two or more fans fail, use the **environment-monitor shutdown fan** command to configure the system to automatically power off the following components:

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

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

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

⚠

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

⚠

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

Examples   The following example shows how to enable fan failure shutdown.

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

Related Commands

Command	Description
show environment	Displays the temperature sensor and fan status.
show hardware	Displays information about the hardware on the shelf.

environment-monitor shutdown temperature

To enable the automatic shutdown of the system if the operating temperature exceeds the critical threshold, use the **environment-monitor shutdown temperature** command. To disable this feature, use the **no** form of the command.

environment-monitor shutdown temperature *slot* /*subslot/module*

no environment-monitor shutdown temperature

Syntax Description		
slot	Specifies a chassis slot.	
subslot	Specifies a chassis sub slot.	
module	Specifies a module.	

Defaults   Enabled

Command Modes   Global configuration

Command History   This table includes the following release-specific history entry:

SV-Release	Modification
12.2(29)SV	This command was introduced.

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

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

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

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

⚠

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

⚠

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

Examples   The following example shows how to enable the automatic shutdown of the system if the operating temperature exceeds the critical threshold:

```
Switch# configure terminal
Switch(config)# environment-monitor shutdown temperature 6/0/0
```

Related Commands

Command	Description
show environment	Displays the temperature sensor and fan status.
environment-monitor temperature-threshold	Changes the default threshold temperatures.

environment-monitor temperature-threshold

To change the default threshold temperatures, use the **environment-monitor temperature-threshold** command. To reset all the thresholds to the default values for all modules, use the **no** form of the command.

environment-monitor temperature-threshold {critical | major | minor | low}
slot/subslot/module <threshold value>

no environment-monitor temperature-threshold

Syntax Description

critical	Specifies the critical alarm.
major	Specifies the major alarm.
minor	Specifies the minor alarm.
low	Specifies the low alarm.
slot	Specifies a chassis slot.
subslot	Specifies a chassis sub slot.
module	Specifies a module.
threshold value	Specifies the new threshold temperature.

Defaults

The following table provides the default threshold temperatures for the alarms:

Alarm	Threshold Temperature in degree Celsius (^{o} C)
Minor	50
Major	60
Critical	70
Low	-15

Command Modes

Global configuration

Command History

This table includes the following release-specific history entry:

SV-Release	Modification
12.2(29)SV	This command was introduced.

Usage Guidelines

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

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

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

Related Commands

Command	Description
show environment	Displays the temperature sensor and fan status.
environment-monitor shutdown temperature	Enables the automatic shutdown of the system if the operating temperature exceeds the critical threshold

hw-module subslot power

To turn off the power to a 2.5-Gbps transponder module in a line card motherboard before removing it, use the **hw-module subslot power** command.

hw-module subslot *slot*/*subcard* **power off**

Syntax Description

slot/*subcard*	Specifies a transponder module in a line card motherboard.
off	Turns off the power to the transponder module.

Defaults   The power to the 2.5-Gbps transponder module is on.

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
12.1(12c)EV2	The **on** option was removed.
SV-Release	Modification
12.2(18)SV	This command was integrated in this release.
S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   When removing a 2.5-Gbps transponder module from the Cisco ONS 15540 ESPx, bit rate errors occur on the transponder modules in the same line card motherboard. These errors do not affect system traffic but they can cause the system to issue alarms if an alarm threshold is exceeded. You can avoid these errors and alarms by turning off the power to the online module with the **hw-module subslot power** command before removing it.

Use the **show hardware linecard** command to display the status of the power to a 2.5-Gbps transponder module.

Note   The **hw-module subslot power** command is only supported on 2.5-Gbps transponder modules installed in line card motherboards with hardware version 5.1, or later, and with LRC (line card redundancy controller) functional image version 2.72, or later.

To determine the functional image and hardware versions on your system, use the **show hardware detail** command.

To power up the transponder module, you must remove it from the line card motherboard and reinsert it.

Examples   The following example shows how to turn the power off to a 2.5-Gbps transponder module before removing it.

```
Switch# hw-module subslot 8/1 power off
Warning: Power OFF subcard 8/1.  Continue? [confirm]y
Switch#
```

Related Commands

Command	Description
show hardware	Shows hardware information.

reload

To reload the active processor card, use the **reload** command.

reload [*text* | **in** [*hh***:**]*mm* [*text*] | **at** *hh***:***mm* [*month day* | *day month*] [*text*] | **cancel**]

Syntax Description	text	Specifies a reason for reloading the active processor card (maximum of 255 characters).
	in [*hh*:]*mm*	Schedules a reload of the software to occur in the specified hours and minutes. The reload must occur within approximately 24 days.
	at *hh:mm*	**Note** The **at** keyword can only be used if the system clock has been set (either through NTP, the hardware calendar, or manually). The time is relative to the configured time zone on the system.
		Schedules a reload of the software to occur at the specified time (using a 24-hour clock).
		If you specify the month and day, the reload is scheduled to occur at that specified time and date. If you do not specify the month and day, the reload occurs at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time).
		Specifying 00:00 schedules the reload for midnight.
		The reload must occur within approximately 24 days.
	month	Specifies the name of the month the reload is to occur, any number of characters in a unique string.
	day	Specifies the number of the day the reload is to occur, in the range 1 to 31.
	cancel	Cancels a scheduled reload.

Defaults   Immediate active processor card reload

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   This command halts the active processor card. If the processor card is set to restart on error, it reboots itself.

Use this command after configuration information is entered into a file and saved to the startup configuration. You cannot reload from a virtual terminal if the processor card is not set up for automatic booting. This prevents the processor card from dropping to the ROM monitor and thereby taking the processor card out of the remote user's control.

If you modify your configuration file, the system prompts you to save the configuration. During a save operation, the system asks you if you want to proceed with the save if the CONFIG_FILE environment variable points to a startup configuration file that no longer exists. If you enter **yes** in this situation, the processor card goes to setup mode upon reload.

When you schedule a reload to occur at a later time, it must occur within approximately 24 days.

This command can be entered on either the active or standby processor card console and only a reload of the processor card on which the command was entered occurs.

When entered on the active processor card, this command synchronizes the running-config to the standby processor card just before the reload is executed, and causes a switchover to the standby processor card only if the standby processor card is in the hot-standby state.

By default the system is configured to reboot automatically, so the active processor card reboots as the standby processor card after the reload.

To display information about a scheduled reload, use the **show reload** command.

Examples   The following example shows how to reload the software on the processor card.

```
Switch# reload
```

The following example reloads the software on the processor card in 10 minutes.

```
Switch# reload in 10
Reload scheduled for 11:57:08 PDT Mon Feb 26 2001 (in 10 minutes)
Proceed with reload? [confirm]
Switch#
```

The following example reloads the software on the processor card at 1:00 p.m. today.

```
Switch# reload at 13:00
Reload scheduled for 13:00:00 PPDT Mon Feb 26 2001 (in 1 hour and 2 minutes)
Proceed with reload? [confirm]
Switch#
```

The following example reloads the software on the processor card on 2/27 at 2:00 a.m.

```
Switch# reload at 02:00 feb 27
Reload scheduled for 02:00:00 PDT Tues Feb 26 2001 (in 38 hours and 9 minutes)
Proceed with reload? [confirm]
Switch#
```

The following example cancels a pending reload.

```
Switch# reload cancel
%Reload cancelled.
```

Related Commands	Command	Description
	config-register	Changes the configuration register settings.
	maintenance-mode	Enables or disables processor card redundancy synchronization.
	redundancy reload peer	Reloads the standby processor card.
	redundancy reload shelf	Reloads both processor cards in the shelf.
	redundancy switch-activity	Manually switches activity from the active processor card to the standby processor card.
	show reload	Displays reload status information.

reprogram

To upgrade the ROMMON or functional image on a selected card from a flash file, use the **reprogram** privileged EXEC command.

> **reprogram** *flash-file-name* {*slot* | **rommon**} [*subcard*]

Syntax Description

flash-file-name	Specifies the name of the image to download, which can be in the CompactFlash Card or bootflash.
slot	Specifies the physical slot number of the controller you want to reprogram. The slot number ranges from 0 to 11.
rommon	Specify reprogramming the ROMMON (ROM monitor) image of the designated CPU switch card.
subcard	Indicate a subcard in a slot for half-width modules or daughter cards in full width cards. The subcard number ranges from 0 to 1.

Defaults   None.

Command Modes   EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   This command reprograms the image to the controller you select. It also resets the selected controller, which causes active connections and configurations to be lost.

⚠
Caution   Do not power cycle the system during a reprogram operation because damage can occur to the controller you are reprogramming. If you power-cycle the system while reprogramming is in progress, you also might be unable to boot the system.

■ reprogram

Examples   The following example shows how to reprogram the image on the processor card in slot 3.

```
Switch# reprogram bootflash:fi-ons15540-muxdemux.A.2-36.exo 3
```

Related Commands

Command	Description
show hardware	Displays information about the programmable device images for a given module in the system.
show upgrade-info functional-image	Displays information from a version diagnotics data file for the ROMMON and functional images on the shelf.

show bootvar

To display boot and related environmental variables for both the active and standby processor cards, use the **show bootvar** command.

>**show bootvar**

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   EXEC and privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   This command shows boot and related information for the active and standby processor cards.

Examples   The following example shows how to display boot information for the system. (See Table 8-1 for field descriptions.)

```
Switch# show bootvar
BOOT variable = bootflash:<imagename>;
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

Standby is up.
Standby BOOT variable = bootflash:<imagename>;
Standby CONFIG_FILE variable =
```

```
Standby BOOTLDR variable =
Standby Configuration register is 0x2
```

Table 8-1   show bootvar Field Descriptions

Field	Description
BOOT variable	Shows a list of bootable images on various devices.
CONFIG_FILE variable	Shows the configuration file used during system initialization.
BOOTLDR variable	Shows the configuration file used during system initialization.
Configuration register	Shows the stored configuration information.
Standby auto-sync startup config mode	Indicates whether startup-config file autosynchronization is enabled or disabled on the standby processor card.
Standby auto-sync running config mode	Indicates whether running-config file autosynchronization is enabled or disabled on the standby processor card.
Standby	Indicates whether the standby processor card is up or down.
Standby BOOT variable	Shows a list of bootable images on various devices for the standby processor card.
Standby CONFIG_FILE variable	Shows the configuration file used during system initialization for the standby processor card.
Standby BOOTLDR variable	Shows the configuration file used during system initialization for the standby processor card.
Standby Configuration register	Shows the stored configuration information for the standby processor card.

Related Commands

Command	Description
auto-sync running-config	Selectively enables only automatic synchronizing of the running configuration to the standby processor card.
auto-sync startup-config	Selectively enables only automatic synchronizing of the startup configuration to the standby processor card.

show ciscoview package

To display Embedded CiscoView package information, use the **show ciscoview package** command.

> **show ciscoview package**

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   EXEC and privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to display Embedded CiscoView package file information or for troubleshooting.

Examples   The following example shows how to display Embedded CiscoView package information. (See Table 8-2 for field descriptions.)

```
Switch# show ciscoview package

File source:slot1:
CVFILE                          SIZE(in bytes)
-----------------------------------------------
ONS15540-1.0.html               8861
ONS15540-1.0.sgz                1183238
ONS15540-1.0_ace.html           3704
ONS15540-1.0_error.html         401
ONS15540-1.0_jks.jar            17003
ONS15540-1.0_nos.jar            17497
applet.html                     8861
cisco.x509                      529
identitydb.obj                  2523
```

Table 8-2   show ciscoview package Field Descriptions

Field	Description
File source	Identifies the slot.
CVFILE	Identifies the Embedded CiscoView files in the package.
SIZE (in bytes)	Shows the file size in bytes.

Related Commands

Command	Description
show ciscoview version	Displays Embedded CiscoView version information.

show ciscoview version

To display Embedded CiscoView version information, use the **show ciscoview version** command.

show ciscoview version

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

EXEC and privileged EXEC

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to display Embedded CiscoView version information.

Examples

The following example shows how to display Embedded CiscoView version information. (See Table 8-3 for field descriptions.)

```
Switch# show ciscoview version

Engine Version: 5.3 ADP Device: ONS15540 ADP Version: 1.0 ADK: 39
```

Table 8-3   show ciscoview version Field Descriptions

Field	Description
Engine Version	Identifies the Embedded CiscoView version.
ADP Device	Identifies the ADP (Autonomous Device Package) device.
ADP Version	Identifies the ADP version.

Related Commands	Command	Description
	show cdl defect-indication	Displays Embedded CiscoView package information.

show environment

To display the temperature sensor and fan status, use the **show environment** command.

show environment

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(12c)EV3	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

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

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

Line card shutdown on fan failure:enabled


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

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

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

Related Commands	Command	Description
	environment-monitor shutdown fan	Enables system shutdown when the fans fail.

show facility-alarm status

To display the facility alarm status, use the **show facility-alarm status** command.

show facility-alarm status [**critical** | **info** | **major** | **minor**]

Syntax Description

critical	Shows the status information for critical facility alarms.
info	Shows the status information for information facility alarms.
major	Shows the status information for major facility alarms.
minor	Shows the status information for minor facility alarms.

Defaults

Displays all facility alarm status information. This information includes external alarms and protocol monitoring alarms.

Command Modes

EXEC and privileged EXEC

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to display the facility alarm and alarm threshold error status information.

Examples

The following example shows how to display the facility alarm status information. (See Table 8-4 for field descriptions.)

```
Switch# show facility-alarm status
System Totals  Critical: 1  Major: 3  Minor: 1
Source: Chassis        Severity: CRITICAL Description: 0    Chassis fan tray missing
Source: Transponder SC  Severity: MAJOR    Description: 0    Access to Tsp card failed
Source: Transponder SC  Severity: MINOR    Description: 1    Access to IDPROM failed
Source: Transponder SC  Severity: MAJOR    Description: 2    Line laser failure detected
Source: Wave2/1/0      Severity: MAJOR    Description: Low alarm threshold exceeded for
Receive Power (in dBm)
```

Cisco ONS 15540 ESPx Command Reference Guide

Table 8-4   show facility-alarm status Field Descriptions

Field	Description
System Totals	Shows the number of alarms in the output display by severity.
Source	Shows the system component that is the source of the alarm.
Severity	Shows the severity of the alarm.
Description	Shows a description of the alarm. If a number is present at the beginning of the description, it is the index of the alarm.

Related Commands

Command	Description
clear facility-alarm	Clears external facility alarm indications.
monitor enable	Enables signal monitoring for certain protocol encapsulations.

show hardware

To display hardware information, use the **show hardware** command.

> **show hardware** [**detail** | **linecard** *slot*]

Syntax Description

detail	Shows detailed hardware information for the entire shelf.
linecard *slot*	Shows detailed hardware information for the motherboard or processor card in a specific slot. The range is 0 to 11.

Defaults   Displays summary hardware information for the entire shelf.

Command Modes   Privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to display hardware information for debugging and tracking.

Examples   The following example shows how to display hardware information for the shelf. (See Table 8-5 for field descriptions.)

```
Switch# show hardware
-------------------------------------------------------------------------------
ONS_15540_Backplane named Switch, Date: 10:25:38 UTC Tue Jul 3 2001
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
Back-Plane Information
-------------------------------------------------------------------------------
Orderable Product No. MAC-Address      MAC-Size Serial No.   Mfg. Date  H/W Ver
-------------------- ---------------- -------- ----------- ---------- -------
15540-CHSA=          00-01-64-45-b1-10 16       TBC05133029 11/02/2001 3.1
```

```
--------------------------------------------------------------------------------
Slot Orderable Product No.    Part No.   Rev Serial No.   Mfg. Date  H/W Ver.
---- ------------------------ ---------- --- ------------ ---------- ----------
0/*  15540-LCMB-UNKNOWN       73-7793-02 11  CAB0604MD7V  2/20/2002  2.0
0/0  15540-MDXA-32AD          05-0893-01 2   402286       11/26/2001 1.0
1/*  15540-LCMB-UNKNOWN       73-7793-02 11  CAB0604MD7A  2/20/2002  1.0
1/0  15540-MDXD-32A0          74-2859-01 2   FE006817     06/21/2001 1.0
2/*  15540-LCMB-1400=         800-17218- 09  CAB06240NF1  10/15/2002 4.1
3/*  15540-TBD                73-7789-01 03  CAB0546L9V5  mm/dd/2001 5.0
3/0  N/A                      68-1345-04 02  CAB0545L8G4  11/15/2001 5.1
3/1  N/A                      68-1345-03 02  CAB0545L8FF  11/15/2001 5.1
4/*  15540-LCMB-1100=         68-1672-03 A0  CAB06310XYC  09/25/2002 2.2
4/0  15540-TSP2-0100=         68-1341-06 A1  CNH0651009F  01/21/2003 5.1
4/2  15540-TSP2-0300=         68-1342-06 A1  CNH0716004N  04/22/2003 5.1
4/3  15540-TSP2-0300=         68-1342-06 A1  CNH0716003V  04/22/2003 5.1
5/*  15540-LCMB-1100          68-1672-02 10  CAB06170BQB  05/29/2002 2.0
5/0  15540-TSP1-25B3=         68-1434-02 B0  CAB0608MQK8  03/23/2002 2.6
5/1  15540-TSP1-25A3=         68-1642-02 B0  CAB061305XQ  07/25/2002 2.6
5/2  15540-TSP1-27A3=         68-1643-02 C0  CAB06190FJY  06/04/2002 2.6
5/3  15540-TSP1-27A3=         68-1643-02 B0  CAB061305QC  07/25/2002 2.6
6/*  N/A                      73-5621-02 03  CAB0505GZHA  02/16/2001 2.5
8/*  15540-LCMB-1100          68-1672-02 10  CAB06192UVB  05/29/2002 2.0
10/* 15540-LCMB-1100          68-1672-02 10  CAB06439NWB  05/29/2002 2.0
10/0 15540-TSP2-0900=         68-1345-06 A1  CNH06430028  11/05/2002 5.1


--------------------------------------------------------------------------------
Power-Supply Module
--------------------------------------------------------------------------------
Power-Supply A is : OK
Power-Supply B is : OK
```

Table 8-5   ***show hardware Field Descriptions***

Field	Description
Slot	Shows the slot or slot and subcard position for the hardware component.
Orderable Product No.	Shows the orderable part number for the component.
Part No.	Shows the part number.
Rev	Shows the revision number.
Serial No.	Shows the serial number.
Mfg. Date	Shows the date the component was manufactured.
H/W Ver.	Shows the hardware version number.

The following example shows how to display detailed hardware information for a specific slot. (See Table 8-6 for field descriptions.)

```
Switch# show hardware linecard 8
--------------------------------------------------------------------------------
Slot Number           : 4/*
Controller Type       : 0x1019
On-Board Description   : ONS_15540_XPS_W/Splitter
Orderable Product Number: 15540-LCMB-1100=
Board Part Number     : 68-1672-03
Board Revision        : A0
Serial Number         : CAB06310XYC
Manufacturing Date    : 09/25/2002
Hardware Version      : 2.2
```

```
RMA Number              : 0
RMA Failure Code        : 0
Functional Image Version: 2.72
Function-ID             : 0
Subcard Power Control   : 0:ON, 1:ON, 2:ON, 3:ON
--------------------------------------------------------------------------------
Slot Number             : 4/0
Controller Type         : 0x1003
On-Board Description     : Type_2_TSP_Ch_1/2_With_Selectable_Client_XVRA
Orderable Product Number: 15540-TSP2-0100=
Board Part Number       : 68-1341-06
Board Revision          : A1
Serial Number           : CNH0651009F
Manufacturing Date      : 01/21/2003
Hardware Version        : 5.1
RMA Number              : 0
RMA Failure Code        : 0
Optical Rx Power Table  : IDPROM based, calibrated
Functional Image Version: 1.A3
Function-ID             : 0
Transceiver type        : Transceiver is absent
--------------------------------------------------------------------------------
Slot Number             : 4/2
Controller Type         : 0x1003
On-Board Description     : Type_2_TSP_Ch_1/2_With_Selectable_Client_XVRA
Orderable Product Number: 15540-TSP2-0300=
Board Part Number       : 68-1342-06
Board Revision          : A1
Serial Number           : CNH0716004N
Manufacturing Date      : 04/22/2003
Hardware Version        : 5.1
RMA Number              : 0
RMA Failure Code        : 0
Optical Rx Power Table  : IDPROM based, calibrated
Functional Image Version: 1.A3
Function-ID             : 0
Transceiver type        : Transceiver is absent
--------------------------------------------------------------------------------
Slot Number             : 4/3
Controller Type         : 0x1003
On-Board Description     : Type_2_TSP_Ch_1/2_With_Selectable_Client_XVRA
Orderable Product Number: 15540-TSP2-0300=
Board Part Number       : 68-1342-06
Board Revision          : A1
Serial Number           : CNH0716003V
Manufacturing Date      : 04/22/2003
Hardware Version        : 5.1
RMA Number              : 0
RMA Failure Code        : 0
Optical Rx Power Table  : IDPROM based, calibrated
Functional Image Version: 1.A3
Function-ID             : 0
Transceiver type        : Transceiver is absent
```

Table 8-6   *show hardware linecard Field Descriptions*

Field	Description
Slot Number	Shows the slot or slot and subcard position for the hardware component.
Controller Type	Shows the hardware component controller type.
On-Board Description	Shows the description stored on the component.

Table 8-6   show hardware linecard Field Descriptions (continued)

Field	Description
Orderable Product Number	Shows the component product order number.
Board Part Number	Shows the part number.
Board Revision	Shows the revision number.
Serial Number	Shows the serial number.
Manufacturing Date	Shows the date the component was manufactured.
Hardware Version	Shows the hardware version number.
RMA Number	Shows the RMA number.
RMA Failure Code	Shows the RMA failure code.
Optical Rx Power Table	Show where the optical receive power calibration is determined.
Functional Image Version	Shows the version of the component functional image.
Subcard Power Control	Shows the status of the power to the subcard positions in the 2.5-Gbps line card motherboard.
Transceiver type	Shows the type of SFP optics installed in a Type 2 extended range transponder module. For SM transponder modules and MM transponder modules, the SFP optics are absent.

Related Commands

Command	Description
environment-monitor shutdown temperature	Controls the power to transponder modules.

show optical wavelength mapping

To display the mapping of Cisco ONS 15540 ESPx channels to ITU grid frequencies and wavelengths, use the **show optical wavelength mapping** command.

show optical wavelength mapping

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   EXEC and privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to display how the Cisco ONS 15540 ESPx channels map to the ITU G.692 grid wavelengths. Channel 0 is the OSC. Channels 1 through 32 are the client data channels. The last two digits of the frequency correspond to the ITU number (for example, the frequency for channel 1 is 192.1 so the ITU grid number is 21).

The frequencies ending in 0 and 5 are missing from the output because they are used as buffers between the 4-channel bands.

Examples   The following example shows how to display wavelength mapping information for the system. (See Table 8-7 for field descriptions.)

```
Switch# show optical wavelength mapping
            Frequency      Wavelength
Channel       (THz)          (nm)
-------     ---------      ----------
   0          191.9         1562.23
   1          192.1         1560.61
   2          192.2         1559.79
```

```
        3          192.3      1558.98
        4          192.4      1558.17
        5          192.6      1556.55
        6          192.7      1555.75
        7          192.8      1554.94
        8          192.9      1554.13
        9          193.1      1552.52
       10          193.2      1551.72
       11          193.3      1550.92
       12          193.4      1550.12
       13          193.6      1548.51
       14          193.7      1547.72
       15          193.8      1546.92
       16          193.9      1546.12
       17          194.1      1544.53
       18          194.2      1543.73
       19          194.3      1542.94
       20          194.4      1542.14
       21          194.6      1540.56
       22          194.7      1539.77
       23          194.8      1538.98
       24          194.9      1538.19
       25          195.1      1536.61
       26          195.2      1535.82
       27          195.3      1535.04
       28          195.4      1534.25
       29          195.6      1532.68
       30          195.7      1531.90
       31          195.8      1531.12
       32          195.9      1530.33
```

Table 8-7   show optical wavelength mapping Field Descriptions

Field	Description
Channel	Identifies the channel.
Frequency (THz)	Shows the frequency for the channel in THz. The last two digits correspond to the ITU grid number.
Wavelength (nm)	Shows the wavelength for the channel in nm.

show temperature

To display shelf temperature information, use the **show temperature** command.

show temperature

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   EXEC and privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to display the current shelf temperature and the alarm threshold temperatures.

Examples   The following example shows how to display internal redundancy software state information. (See Table 8-8 for field descriptions.)

```
Switch> show temperature
   Sensor             Temperature            Thresholds
                      (degree C)    Minor    Major    Critcal   Low
-------------------   ----------   ------------------------------------
Inlet Sensor             31          65       75         80      -15
Outlet Sensor            33          75       85         90      -15

   Sensor                   Alarms
                      Minor   Major   Critical
-------------------   ------------------------
Inlet Sensor            0       0         0
Outlet Sensor           0       0         0
```

Table 8-8   show temperature Field Descriptions

Field	Description
Sensor	Shows the type of sensor.
Temperature (degree C)	Shows the current temperature in degrees Celsius.
Minor	Shows temperature threshold that generates a minor alarm.
Major	Shows temperature threshold that generates a major alarm.
Critical	Shows temperature threshold that generates a critical alarm.
Low	Shows temperature threshold that generates a low alarm.
Alarms	Shows the number of minor, major, and critical alarms on the inlet and outlet sensors.

Related Commands

Command	Description
show facility-alarm status	Shows the facility alarm status information.

show upgrade-info functional-image

To display ROMMON and functional image version diagnotics, use the **show upgrade-info functional-image** command.

> **show upgrade-info functional-image** {**all** | **latest-version** [**software-compatible**]} **dat-file** *device***:***filename* [**detail**]

Syntax Description

all	Displays information about all the functional images found in the data file.
latest-version	Displays information about the latest functional images on the system.
software-compatible	Displays information about the latest functional images which are compatible with the currently running system image.
dat-file *device***:***filename*	Specifies the name of the data file containing the version diagnostics for the ROMMON and functional images on the system.
detail	Displays detailed functional image version diagnotics.

Defaults

None

Command Modes

Privileged EXEC

Command History

This table includes the following release-specific history entries:

- SV-Release
- S-Release

SV-Release	Modification
12.2(18)SV	This command was first introduced.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to display the version diagnotics for ROMMON and functional images. The data file to use in conjunction with this command can be downloaded from the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/ons15540-fpga

The following example shows how to display detailed APS information for all APS groups. (See Table 8-9 for field descriptions.)

```
Switch# show upgrade-info functional-image all dat-file
bootflash:fi-ons15540-index.008.dat
Validating CRC...100%

Generating Functional Image Upgrade Information for the currently running IOS
using DAT file bootflash:fi-ons15540-index.008.dat, created on Tues Aug 19 00:20:15 PST
2003.
```

```
Please ensure that you are using the latest DAT file from
Cisco Connection Online (CCO) Webpage

Abbr: Cur.FV = Functional Image Version of the Card.
      Lis.FV = List of Func. Image Versions found in the DAT-file for the
               corresponding card.
      (U)    = IOS Software upgrade is required, to upgrade to
               the recommended functional image version.

Slot Product No                Cur.FV Lis.FV Listed Functional Image
---- ------------------------ ------ ------ ------------------------------
 0/* 15540-LCMB-UNKNOWN         2.66   2.66  No Func. Image Upgrade Required
 1/* 15540-LCMB-UNKNOWN         2.67   2.67  No Func. Image Upgrade Required
 3/* 15540-LCMB-1100            2.72   2.72  No Func. Image Upgrade Required
 3/0 15540-TSP2-0100=           1.F1   1.F1  No Func. Image Upgrade Required
 3/1 15540-TSP2-0100=           1.F1   1.F1  No Func. Image Upgrade Required
 3/3 15540-TSP1-13B3=           1.F1   1.F1  No Func. Image Upgrade Required
 4/0 15540-LCMB-1100            1.A0   1.A1  fi-ons15540-tlcmdb.A.1-A1.exo
 6/* 15540-CPU=                 1.25   1.27  fi-ons15540-ph0cpu.A.1-27.exo
 7/* 15540-CPU=                 1.27   1.27  No Func. Image Upgrade Required
```

Table 8-9   *show upgrade-info functional-image Field Descriptions*

Field	Description
Slot	Indicates the slot for a card and the slot and subcard for a module.
Product No	Indicates the product number for the card or module.
Cur. FV	Indicates the current ROMMON or functional image version on the card or module.
Lis. FV	Indicates the ROMMON or functional image version listed in the data file.
Listed Function Image	Indicates the name of the ROMMON or functional image file to use to upgrade the card or module.

Related Commands

Command	Description
reprogram	Updates the ROMMON or functional image on a card or module.
show hardware	Displays information about the hardware on the shelf.

show version

To display the system hardware configuration, software version, and names and sources of configuration files and boot images, use the **show version** command.

> **show version**

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   EXEC and privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to display the system hardware configuration, software version, and names and sources of configuration files and boot images.

> **Note**   Always specify the complete software version number when reporting a possible software problem.

Examples   The following example shows how to display version information for the system. Table 8-10 describes the output from the **show version** command.

```
Switch# show version

 Cisco Internetwork Operating System Software
 IOS (tm) ONS-15540 Software (manopt-M0-M), Experimental Version 12.1(20001031:221042)
[ffrazer-man_cosmos 252]
 Copyright (c) 1986-2001 by cisco Systems, Inc.
 Compiled Fri 23-Feb-01 15:23 by ffrazer
 Image text-base:0x60010950, data-base:0x604E8000
```

```
  ROM:System Bootstrap, Version 12.1(20001031:194138) [ffrazer-man_cosmos 233],
DEVELOPMENT SOFTWARE
  BOOTFLASH:ONS-15540 Software (manopt-M0-M), Experimental Version 12.1(20001031:221042)
[ffrazer-man_cosmos 246]

  Switch uptime is 30 minutes
  System returned to ROM by power-on
  System image file is "tftp://171.69.1.129/ffrazer/manopt-m0-mz.010223.6"

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

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

  20480K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
  16384K bytes of Flash internal SIMM (Sector size 64K).
  Configuration register is 0x102
```

Table 8-10   show version Field Descriptions

Field	Description
Software version	Shows the software version.
Compiled	Shows the date and time the software was compiled.
System Bootstrap, Version	Shows the system bootstrap version number.
BOOTFLASH, Version	Shows the bootflash version number.
Switch uptime	Shows the number of days, hours, minutes, and seconds the system has been up and running.
System returned to ROM by power-on	Shows how the system was last booted—as a result of a normal system startup or because of system error.
System image file	Shows the name and location of the system image file.
bytes of memory	Shows the amount of system memory.
Last reset from power-on	Shows how the system was last reset.
2 Ethernet/IEEE 802.3 interface(s)	Shows the number, type, and encapsulation of interfaces available.
non-volatile configuration memory	Shows the amount of nonvolatile configuration memory available.
Flash PCMCIA	Shows the amount of Flash memory and location of the card.
Flash internal SIMM	Shows the amount of Flash internal SIMM memory.
Configuration register	Shows the location of the configuration register.

traceroute

To trace the IP routes the packets actually take when traveling from the Cisco ONS 15540 ESPx NME (network management Ethernet) port to their destination, use the **traceroute** EXEC command.

EXEC Mode

> **traceroute** *protocol destination*

Privileged EXEC Mode

> **traceroute** [*protocol*] [*destination*]

Syntax Description		
protocol	Protocols that can be used are **appletalk**, **clns**, **ip**, **ipx**, and **vines**.In privileged EXEC mode, the default protocol is assumed for the destination address format.
destination	Destination address or host name on the command line. In privileged EXEC mode, the default parameters for the appropriate protocol are assumed.

Defaults   The *protocol* argument is based on the format of the *destination* argument. For example, if the system finds a destination in IP format, the protocol defaults to **ip**.

Command Modes   EXEC and privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   The **traceroute** command works by taking advantage of the error messages generated by the system when a datagram exceeds its TTL (Time To Live) value. The **traceroute** command starts by sending probe datagrams with a TTL value of 1. This causes the first system to discard the probe datagram and send back an error message. The **traceroute** command sends several probes at each TTL level and displays the round-trip time for each.

The **traceroute** command sends out one probe at a time. Each outgoing packet may result in one or two error messages. A `time exceeded` error message indicates that an intermediate system detected and discarded the probe. A `destination unreachable` error message indicates that the destination node received and discarded the probe because it could not deliver the packet. If the timer goes off before a response comes in, **traceroute** prints an asterisk(*).

The **traceroute** command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with the escape sequence. By default, to invoke the escape sequence, enter **^X**.

Common Trace Problems

Due to bugs in the IP implementation of various hosts and switches, the IP **traceroute** command may behave in unexpected ways.

Not all destinations respond correctly to a probe message by sending back an `ICMP port unreachable` message. A long sequence of TTL levels with only asterisks, terminating only when the maximum TTL is reached, may indicate this problem.

There is a known problem with the way some hosts handle an `ICMP TTL exceeded` message. Some hosts generate an ICMP message, but they reuse the TTL of the incoming packet. Because this is zero, the ICMP packets do not make it back. When you trace the path to such a host, you may see a set of TTL values with asterisks (*). Eventually, the TTL gets high enough that the ICMP message can get back. For example, if the host is 6 hops away, **traceroute** times out in responses 6 through 11.

Examples   The following example displays sample IP **traceroute** output in EXEC mode when a destination host name is specified. (See Table 8-11 for field descriptions.)

```
Switch> traceroute ip ABA.NYC.mil

Type escape sequence to abort.
Tracing the route to ABA.NYC.mil (26.0.0.73)
        1 DEBRIS.CISCO.COM (131.108.1.6) 1000 msec 8 msec 4 msec
        2 BARRNET-GW.CISCO.COM (131.108.16.2) 8 msec 8 msec 8 msec
        3 EXTERNAL-A-GATEWAY.STANFORD.EDU (192.42.110.225) 8 msec 4 msec 4 msec
        4 BB2.SU.BARRNET.NET (131.119.254.6) 8 msec 8 msec 8 msec
        5 SU.ARC.BARRNET.NET (131.119.3.8) 12 msec 12 msec 8 msec
        6 MOFFETT-FLD-MB.in.MIL (192.52.195.1) 216 msec 120 msec 132 msec
        7 ABA.NYC.mil (26.0.0.73) 412 msec 628 msec 664 msec
```

Table 8-11   traceroute command Field Descriptions

Field	Description
1	Indicates the sequence number of the system in the path to the host.
DEBRIS.CISCO.COM	Shows the host name of this system.
131.108.1.61	Shows the IP address of this system.
1000 msec 8 msec 4 msec	Shows the round-trip time for each of the three probes that are sent.

Table 8-12 describes the characters that can appear in **traceroute** output.

Table 8-12   IP Trace Text Characters

Character	Description
nn msec	Indicates for each node the round-trip time in milliseconds for the specified number of probes.
*	Indicates that the probe timed out.
?	Indicates an unknown packet type.
Q	Indicates a source quench.
P	Indicates that the protocol is unreachable.
N	Indicates that the network is unreachable.
U	Indicates that the port is unreachable.
H	Indicates that the host is unreachable.

The following example displays sample IP **traceroute** output in privileged EXEC mode when a destination IP address is specified. (SeeTable 8-13 for prompt descriptions and Table 8-11 for field descriptions.)

```
Switch# traceroute
Protocol [ip]:
Target IP address: 10.0.0.1
Source address:
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 10.0.0.1

  1 10.0.0.2 msec 0 msec 4 msec
  2 10.0.1.9 0 msec 0 msec 0 msec
  3 10.0.0.1 0 msec 0 msec 4 msec
```

Table 8-13   traceroute Command Prompt Descriptions

Prompt	Description
Protocol [ip]:	Specifies the protocol. The default is IP.
Target IP address:	Specifies the host name or an IP address. There is no default.
Source address:	Specifies one of the interface addresses of the router to use as a source address for the probes. The system will normally pick what it feels is the best source address to use.
Numeric display [n]:	Specifies the **traceroute** display format. The default is to have both a symbolic and numeric display; however, you can suppress the symbolic display.
Timeout in seconds [3]:	Specifies the number of seconds to wait for a response to a probe packet. The default is 3 seconds.
Probe count [3]:	Specifies the number of probes to be sent at each TTL level. The default count is 3.

Table 8-13   *traceroute Command Prompt Descriptions (continued)*

Prompt	Description
Minimum Time to Live [1]:	Specifies the TTL value for the first probes. The default is 1, but it can be set to a higher value to suppress the display of known hops.
Maximum Time to Live [30]:	Specifies the largest TTL value that can be used. The default is 30. The **traceroute** command terminates when the destination is reached or when this value is reached.
Port Number [33434]:	Specifies the destination port used by the UDP probe messages. The default is 33434.
Loose, Strict, Record, Timestamp, Verbose [none]:	Specifies the IP header options. You can specify any combination. The **traceroute** command issues prompts for the required fields. Note that trace will place the requested options in each probe; however, there is no guarantee that all routers (or end nodes) will process the options. The default is no header options. The options are: • Loose—Allows you to specify a list of nodes that must be traversed when going to the destination. • Strict—Allows you to specify a list of nodes that must be the only nodes traversed when going to the destination. • Record—Allows you to specify the number of hops to leave room for. • Timestamp—Allows you to specify the number of time stamps to leave room for. • Verbose—If you select any of the above options, the verbose mode is automatically selected and the **traceroute** command prints the contents of the option field in any incoming packets. You can prevent verbose mode by selecting it again, toggling its current setting.

Threshold Commands

Interface alarm thresholds provide a way to monitor the quality of the client signal. Use the following commands to configure and monitor interface alarm threshold operations.

aps trigger

To enable y-cable line card protection signal switchover when the alarm thresholds are exceeded, use the **aps trigger** command. To disable y-cable protection signal switchover, use the **no** form of this command.

aps trigger

no aps trigger

Syntax Description   This command has no other arguments or keywords.

Defaults   Disabled

Command Modes   Threshold configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command in a y-cable protection configuration to cause a signal switchover when the active signal error rates exceed the alarm thresholds. The signal switchover occurs only if the standby signal is acceptable.

Note   The threshold list must be applied to both interfaces in the associated pair.

Examples   The following example shows how to configure an APS switchover trigger for an alarm threshold.

```
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 chicago
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)# aps enable
Switch(config-red-aps)# exit
Switch(config-red)# exit
Switch(config)# interface transparent 3/0/0
Switch(config-if)# encap sonet oc3
Switch(config-if)# monitor enable
Switch(config-if)# threshold-group sonet-alarms
Switch(config-if)# exit
Switch(config)# interface transparent 5/0/0
Switch(config-if)# encap sonet oc3
Switch(config-if)# monitor enable
Switch(config-if)# threshold-group sonet-alarms
```

Related Commands	Command	Description
	monitor enable	Enables protocol performance monitoring.
	show threshold-list	Displays the contents of a threshold list.
	threshold	Selects alarm threshold to modify and enters threshold configuration mode.
	threshold-group	Associates a threshold list to an interface.
	threshold-list	Creates a threshold list with a name or allows an existing list to be modified. Switches from configuration mode to threshold-list configuration mode.

description

To configure a alarm threshold description, use the **description** command. To remove a threshold description, use the **no** form of the command.

description *text*

no description

Syntax Description

text	Threshold description for the MIB.

Defaults   None

Command Modes   Threshold configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   First use the **threshold-list** command to enter threshold list configuration mode and create a threshold list. Then use the **threshold** command to specify a threshold to modify and enter threshold configuration mode. This description can be accessed and displayed by network management systems that support SNMP.

Examples   The following example shows how to create a description for a threshold in a threshold list named temp.

```
Switch# configure terminal
Switch(config)# threshold-list temp
Switch(config-t-list)# threshold name sonet-sdh section cv degrade
Switch(config-threshold)# description This threshold is for SONET and SDH BIP1 errors
```

Related Commands

Command	Description
threshold	Selects alarm threshold to modify and enters threshold configuration mode.
threshold-group	Associates a threshold list with an interface.
threshold-list	Creates a threshold list with a name or allows an existing list to be modified. Switches from configuration mode to threshold-list configuration mode.

notification-throttle timer

To modify the alarm threshold notification throttle timer, use the **notification-throttle timer** command. To return the notification throttle timer interval to its default value, use the **no** form of the command.

notification-throttle timer *seconds*

no notification-throttle timer

Syntax Description

seconds	Specifies, in seconds, the interval in which no more than one threshold alarm notification can be generated. If more than one notification is generated during the hold-down period, the extra notifications are delayed. The range is 5 to 500 seconds.

Defaults

5 seconds

Command Modes

Threshold list configuration

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to control the amount of alarm threshold notification activity that is generated on the system.

Examples

The following example shows how to set an alarm threshold list notification throttle timer to 10 seconds.

```
Switch# configure terminal
Switch(config)# threshold-list sonet-alarms
Switch(config-t-list)# notification-throttle timer 10
```

Related Commands

Command	Description
show threshold-list	Displays the contents of a threshold list.
threshold-list	Groups a set of thresholds with a name. Switches from configuration mode to threshold-list configuration mode.

show threshold-list

To display information about alarm threshold lists, use the **show threshold-list** command.

show threshold-list [*name*]

Syntax Description

name	Specifies the name of an alarm threshold list.

Defaults

Displays information about all threshold lists in the system.

Command Modes

EXEC and privileged EXEC

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to display the threshold values configured for all alarm threshold lists or for a specific alarm threshold list.

Examples

The following example shows how to display information for an alarm threshold list named sonet-counters. (See Table 9-1 for field descriptions.)

```
Switch# show threshold-list

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
```

Table 9-1   show threshold-list Field Descriptions

Field	Description
Threshold List Name	Shows the name of the threshold list.
Notification throttle timer	Shows, in seconds, the interval in which no more than one threshold alarm notification can be generated. If more than one notification is generated during the hold-down period, the extra notifications are delayed.
Threshold name	Shows the name of the threshold counter. See the **threshold** command for a list of threshold names.
Severity	Shows the threshold severity (Degrade or Failure).
Value	Shows the threshold rate value for the system to issue an alarm.
APS Trigger	Indicates whether the APS switchover trigger is set.
Description	Shows the description text for the counter.

Related Commands

Command	Description
aps trigger	Enables APS switchover trigger for threshold alarms.
description	Configures MIB description for threshold alarms.
notification-throttle timer	Modifies the alarms threshold notification throttle timer.
snmp-server enable traps threshold min-severity	Enables SNMP trap notification for threshold alarms.
threshold	Selects alarm threshold to modify and enters threshold configuration mode.
threshold-group	Associates a threshold list to an interface.
threshold-list	Creates a list of thresholds.
value	Configures the value for threshold alarms.

threshold

To configure an alarm threshold in a threshold list, use the **threshold** command. To remove a threshold from a threshold list, use the **no** form of the command.

threshold name {**cvrd** | **cdl hec** | **crc** | **sonet-sdh section cv** | **tx-crc**} {**degrade** | **failure**} [**index** *value*]

no threshold name {**cvrd** | **cdl hec** | **crc** | **sonet-sdh section cv** | **tx-crc**} {**degrade** | **failure**} [**index** *value*]

Syntax Description		
cvrd	Specifies the coding violation and running disparity counter. This counter is monitored for interfaces with the following encapsulation:	
	• Gigabit Ethernet	
	• ESCON	
	• Fibre Channel	
	• FICON	
cdl hec	Specifies the CDL (converged data link) HEC (header error control) error counter. This counter is monitored for wave interfaces that insert and delete CDL headers.	
crc	Specifies the cyclic redundancy error counter.	
sonet-sdh section cv	Specifies the bit interleaved parity error. This counter is monitored for interfaces with either SONET or SDH encapsulation.	
tx-crc	Specifies the transmit cyclic redundancy error counter.	
degrade	Specifies that a signal degrade threshold alarm is generated.	
failure	Specifies that a signal failure threshold alarm is generated.	
index *value*	Specifies a MIB index. The range is 0 to 63.	

Defaults   None

Command Modes   Threshold-list configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**

12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   First use the **threshold-list** command to enter threshold-list configuration mode and create a threshold list. Then use the **threshold** command to enter threshold configuration mode for the specific threshold. In threshold configuration mode, you can modify the threshold attribute values.

Interfaces have no default alarm threshold values. When monitoring is enabled, alarm thresholds are only in effect when a threshold list is associated with the interface.

By default, the **threshold** command uses the next available threshold index number in the threshold list MIB. The **index** keyword and value allow you to explicitly assign an index for the threshold. This is particularly useful as index numbers become available when thresholds are deleted.

Examples   The following example shows how to configure an alarm threshold in a threshold list and enter threshold configuration mode.

```
Switch# configure terminal
Switch(config)# threshold-list temp
Switch(config-t-list)# threshold name cvrd degrade
Switch(config-threshold)#
```

Related Commands

Command	Description
aps trigger	Enables APS switchover when the alarm threshold is crossed.
description	Specifies a threshold description for the SNMP MIB.
notification-throttle timer	Modifies the alarm threshold notification throttle timer.
show threshold-list	Displays the contents of a threshold list.
snmp-server enable traps threshold min-severity	Enables SNMP trap notifications for alarm threshold activity.
threshold-group	Associates a threshold list to an interface.
threshold-list	Groups a set of thresholds with a name. Switches from configuration mode to threshold-list configuration mode.
value	Specifies the threshold value.

threshold-group

To associate a threshold list to an interface, use the **threshold-group** command. To remove a threshold list from an interface, use the **no** form of this command.

threshold-group *name*

no threshold-group *name*

Syntax Description

name	Specifies the name of a threshold list and associates it with a specified interface.

Defaults   None

Command Modes   Interface configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to associate a threshold list to a specified interface.

Even though a threshold list might contain the thresholds for all error counters, not all of these thresholds are applicable to the interface. Thresholds are recognized by the interface based on the interface type (for example, wave or waveethernetphy) and the encapsulation type (in the case of transparent interfaces).

You can associate more than one threshold list with an interface. The lists cannot contain overlapping thresholds. The system will not allow you to associate a threshold list if it contains a counter the interface already monitors for another threshold list.

If the interface is not associated with any threshold list, the threshold counters that are monitored on that interface are set to their default values.

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

Examples The following example shows how to associate a threshold list to a transparent interface.

```
Switch# configure terminal
Switch(config)# interface transparent 2/0/0
Switch(config-if)# threshold-group temp
```

Related Commands

Command	Description
show threshold-list	Displays the contents of a threshold list.
threshold	Creates failure and degrade thresholds for different error counters that are monitored on the interface.
threshold-list	Creates a threshold list with a name or allows an existing list to be modified. Switches from configuration mode to threshold-list configuration mode.

threshold-list

To create a list of thresholds, or modify an existing threshold list, use the **threshold-list** command. To delete the threshold list, use the **no** form of this command.

threshold-list *name*

no threshold-list *name*

Syntax Description	name	Specifies the name of the threshold list to be created and associated with a specified interface. The list name cannot begin with the text string "default".

Defaults   None

Command Modes   Global configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to create a list, or modify an existing list, of signal degrade and signal failure alarm thresholds for monitored error counters. After entering the command, the CLI enters threshold configuration mode where you can specify the threshold list attributes or threshold counters to add or modify.

Before deleting or modifying a threshold list, remove it from all the interfaces that use it.

Examples   The following example shows how to create a threshold list called temp.

```
Switch# configure terminal
Switch(config)# threshold-list temp
Switch(config-t-list)#
```

Related Commands

Command	Description
aps trigger	Enables APS switchover when the alarm threshold is crossed.
description	Specifies a threshold description for the SNMP MIB.
notification-throttle timer	Modifies the alarm threshold notification throttle timer.
show threshold-list	Displays the contents of a threshold list.
snmp-server enable traps threshold min-severity	Enables SNMP trap notifications for alarm threshold activity.
threshold	Creates failure and degrade thresholds for different error counters that are monitored on the interface.
threshold-group	Associates a threshold list to an interface.
value	Specifies the threshold value.

value

To configure the values of failure and degrade alarm threshold rates, use the **value** command. To remove an threshold rate, use the **no** form of the command.

value rate *value*

no value

Syntax Description

rate *value*	Enters the threshold value as 10^{-x}, where *value* is x in 10^{-x}. The range is 3 to 9.

Defaults   None

Command Modes   Threshold configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   First use the **threshold-list** command to enter threshold-list configuration mode and create a threshold list. Then use the **threshold** command to specify a threshold to modify and enter threshold configuration mode.

The degrade rate value for a threshold must always be less than the failure rate value. For example, if the failure rate for a threshold is 7, or 10^{-7}, then the degrade value must be 8 or 9.

Table 9-2 lists the errors per second for the threshold rates for each of the protocol encapsulations.

Table 9-2   Thresholds for Monitored Protocols (Errors Per Second)

Rate	10 Gigabit Ethernet CVRD	10 Gigabit Ethernet CDL HEC	SONET OC-3 or SDH STM-1	SONET OC-12 or SDH STM-4	SONET OC-48 or SDH STM-16	Gigabit Ethernet	ESCON	FICON	Fibre Channel[1]	ISC[2]
3	12,443,900	6512	31,753[3]	32,000[3]	32,000[3]	1,244,390	199,102	1,057,731	1,057,731	1,057,731
4	1,249,438	665	12,318	27,421	31,987[3]	124,944	19,991	106,202	106,202	106,202
5	124,944	67	1518	56,54	17,296	12,499	2000	10,625	10,625	10,625
6	10,312	7	155	616	2394	1250	200	1062	1062	1062
7	1031	0.7	15.5	62	248	125	20	106	106	106
8	103	0.07	1.55	6.2	24.8	12.5	2	10.6	10.6	10.6
9	10	0.007	0.155	0.62	2.48	1.25	0.2	1.06	1.06	1.06

1. Only 1 Gbps rate is supported.

2. Compatibility mode only.

3. Rate is limited by the hardware.

Examples   The following example shows how to create thresholds within a threshold list (temp) with the SONET and SDH section code violation error threshold signal degrade rate of 9 and signal failure rate of 7.

```
Switch# configure terminal
Switch(config)# threshold-list temp
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)# end
Switch#
```

Related Commands

Command	Description
threshold	Selects alarm threshold to modify and enters threshold configuration mode.
threshold-group	Associates a threshold list with an interface.
threshold-list	Creates a threshold list with a name or allows an existing list to be modified. Switches from configuration mode to threshold-list configuration mode.

■   **value**

Topology Neighbor Commands

Use the following commands to configure and monitor network topology neighbors.

show topology

To display information about the global physical network topology configuration, use the **show topology** command.

show topology

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   EXEC and privileged EXEC

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to display the global physical network topology configuration information.

Examples   The following example shows how to display the topology hold-time interval. (See Table 10-1 for field descriptions.)

```
Switch# show topology
Global Physical Topology configuration:
  Maximum Hold Time = 300 secs
  Trap interval = 60 secs
```

Table 10-1   show topology hold-time Field Descriptions

Field	Description
Maximum Hold Time	Shows the maximum number of seconds a dynamically generated topology entry will remain before it times out.
Trap interval	Shows the number of seconds for the topology SNMP trap notification throttle interval.

Related Commands

Command	Description
show topology neighbor	Displays network topology information.
snmp-server enable traps topology	Configures the network topology SNMP trap notification throttle interval.
topology hold-time	Modifies the interval to hold a nonstatic topology node entry.

show topology neighbor

To display the network topology neighbors for the shelf, use the **show topology neighbor** command.

show topology neighbor [**detail**]

Syntax Description

detail	Shows the agent IP address and how the topology entry was created.

Defaults

Displays summary information.

Command Modes

Privileged EXEC

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to display the network topology neighbors for the shelf.

Examples

The following example shows how to display network topology neighbor information for the shelf. (See Table 10-2 for field descriptions.)

```
Switch# show topology neighbor
Physical Topology:

Local Port    Neighbor Node    Neighbor Port
----------    -------------    -------------
Wd0/3         Switch2          Wd0/0
```

Table 10-2   show topology neighbor Field Descriptions

Field	Description
Local Port	Identifies the local port.

Table 10-2   show topology neighbor Field Descriptions (continued)

Field	Description
Neighbor Node	Identifies the neighbor node.
Neighbor Port	Identifies the port or wdm interface on the neighbor node.

The following example shows how to display detailed network topology neighbor information for the shelf. (See Table 10-3 for field descriptions.)

```
Switch# show topology neighbor detail
Physical Topology:

Local Port: Wdm0/3
Neighbor Node        : Switch2
Neighbor Port        :
Neighbor Agent Address: 172.20.54.159
Neighbor Discovery    : Via CDP (Proxy Port: Wave0)
```

Table 10-3   show topology neighbor detail Field Descriptions

Field	Description
Local Port	Identifies the local port.
Neighbor Node	Identifies the neighbor node.
Neighbor Port	Identifies the port on the neighbor node.
Neighbor Agent Address	Identifies the IP address of the topology agent on the neighbor node.
Neighbor Discovery	Indicates how the topology neighbor was discovered, either automatically through CDP or manually through the CLI.

Related Commands

Command	Description
show topology	Displays global physical topology configuration.
snmp-server enable traps topology	Configures the network topology SNMP trap notification throttle interval.
topology neighbor	Adds a static entry for an interface to the network topology.
topology neighbor agent ip-address	Specifies the network management agent address on a remote node.
topology neighbor cdp	Enables CDP on wdm interfaces.
topology neighbor disable	Removes an interface from the network topology.
topology hold-time	Modifies the interval to hold a nonstatic topology node entry.

topology hold-time

To modify the interval to hold nonstatic topology node entries, use the **topology hold-time** command. To return the hold-time interval to its default value, use the **no** form of the command.

topology hold-time *seconds*

no topology hold-time

Syntax Description

seconds	Specifies the number of seconds. The range is 1 to 2147483647 seconds.

Defaults

300 seconds

Command Modes

Global configuration

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to modify the network topology hold-time timer interval. This timer helps avoid reconstructing a nonstatic topology entry when a node leaves the network for only a brief time.

Examples

The following example shows how to modify the network topology hold time.

```
Switch# configure terminal
Switch(config)# topology hold-time 60
```

Related Commands	Command	Description
	show topology	Displays global physical topology configuration.
	snmp-server enable traps topology	Configures the network topology SNMP trap notification throttle interval.
	topology neighbor cdp	Enables CDP on wdm interfaces.

topology neighbor

To manually add a static entry for a thru, OSC wave, oscfilter, tengigethernetphy, transparent, wdm, or wdmsplit interface to the network topology, use the **topology neighbor** command. To remove the interface from the network topology, use the **no** form of the command or the **topology neighbor disable** command.

> **topology neighbor** {**name** *node-name* | **ip-address** *ip-address* |
>   **mac-address** *mac-address*} {**port name** *port-name* | **port ip-address** *port-ip-address* |
>   **port mac-address** *port-mac-address*} [transmit | receive]

> **no topology neighbor** {**name** *node-name* | **ip-address** *ip-address* |
>   **mac-address** *mac-address*} {**port name** *port-name* | **port ip-address** *port-ip-address* |
>   **port mac-address** *port-mac-address*} [transmit | receive]

Syntax Description

name *node-name*	Specifies the name of the neighbor node.
ip-addess *ip-address*	Specifies the IP address of the neighbor node.
mac-addess *mac-address*	Specifies the MAC address of the neighbor node.
port name *port-name*	Specifies the name of the port on the neighbor node.
port ip-address *port-ip-address*	Specifies the IP address of the port on the neighbor node.
port mac-address *port-mac-address*	Specifies the MAC address of the port on the neighbor node.
transmit	Indicates that the link to the neighbor is transmit only.
receive	Indicates that the link to the neighbor is receive only.

Defaults   CDP (Cisco Discovery Protocol) is enabled on wdm interfaces.

Both directions.

No topology is configured on transparent or wdmsplit interfaces.

Command Modes   Interface configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
12.1(12c)EV	Support for wdmrelay interfaces was added.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to manually add wdm, thru, oscfilter, OSC wave, tengigethernetphy, transparent, and wdmsplit interfaces to the network topology. You must also configure the network management agent IP address with the **topology neighbor agent ip-address** command. By default, CDP is enabled on all these interface types.

For transparent interfaces, you must use the **topology neighbor** command to add the interface to the network topology because the transparent interfaces do not support CDP. For wdm interfaces, use either the **topology neighbor** command or the **topology neighbor cdp** command to populate the network topology.

For wdmsplit interfaces, you must use the **topology neighbor** command to add both the west and east interfaces on the PSM to the network topology.

For y-cable protected configurations, add both associated transparent interfaces to the network topology.

You can also use the **topology neighbor disable** command to remove an interface from the network topology.

Use the direction option to distinguish between bidirectional link neighbors and unidirectional (transmit or receive) link neighbors.

Examples

The following example shows how to connect a mux/demux module to a mux/demux module in another node.

```
Switch# configure terminal
Switch(config)# interface wdm 0/2
Switch(config-if)# topology neighbor name NodeA port name wdm0/0
Switch(config-if)# topology neighbor agent ip-address 10.1.1.1
```

The following example shows how to connect a transponder module to an interface on the client equipment.

```
Switch# configure terminal
Switch(config)# interface transparent 2/0/2
Switch(config-if)# topology neighbor name Router1 port name gigabitethernet2/1
Switch(config-if)# topology neighbor agent ip-address 10.2.2.2
```

The following example shows how to connect a PSM to a PSM on another node.

```
Switch# configure terminal
Switch(config)# interface wdmsplit 0/1/0
Switch(config-if)# topology neighbor name NodeB port name wdmsplit0/1/0
Switch(config-if)# topology neighbor agent ip-address 10.3.3.3
```

Related Commands

Command	Description
show topology neighbor	Displays network topology information.
snmp-server enable traps topology	Enables SNMP trap notifications for the network topology.
topology neighbor agent ip-address	Specifies the network management agent IP address.

Command	Description
topology neighbor cdp	Enables CDP on wdm interfaces.
topology neighbor disable	Removes the interface from the network topology.

topology neighbor agent ip-address

To specify the network management agent address on a remote node, use the **topology neighbor agent ip-address** command. To remove the network management agent address from an interface, use the **no** form of the command.

topology neighbor agent ip-address *ip-address* [transmit | receive]

no topology neighbor agent ip-address *ip-address* [transmit | receive]

Syntax Description

ip-address	Specifies the IP address of the network management agent on the neighbor node. This address is usually the IP address configured on the NME interface on the neighbor node.
transmit	Indicates that the link to the neighbor is transmit only.
receive	Indicates that the link to the neighbor is receive only.

Defaults   Both directions

Command Modes   Interface configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
12.1(12c)EV	Support for wdmrelay interfaces was added.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command if you have configured a network topology manually with the **topology neighbor** command.

The network management agent IP address is usually the IP address of the NME on the node.

Note   Do not use this command if you have enabled CDP on the interface with the **topology neighbor cdp** command.

Examples   The following example shows how to configure a network management agent on a wdm interface.

```
Switch# configure terminal
Switch(config)# interface wdm 0/2
Switch(config-if)# topology neighbor name NodeA port name wdm0/0
Switch(config-if)# topology neighbor agent ip-address 209.165.202.129
```

The following example shows how to configure a network management agent on a transparent interface.

```
Switch# configure terminal
Switch(config)# interface transparent 2/3/0
Switch(config-if)# topology neighbor name Router2 port name gigabitethernet2/2
Switch(config-if)# topology neighbor agent ip-address 209.165.202.130
```

The following example shows how to configure a network management agent on a wdmsplit interface.

```
Switch# configure terminal
Switch(config)# interface transparent 0/1/1
Switch(config-if)# topology neighbor name NodeB port name wdmsplit0/1/1
Switch(config-if)# topology neighbor agent ip-address 209.165.202.131
```

Related Commands

Command	Description
show topology neighbor	Displays the topology configuration.
topology neighbor	Adds a static entry for an interface to the network topology.

topology neighbor cdp

To enable CDP topology discovery on wdm and tengigethernetphy interfaces, use the **topology neighbor cdp** command. To disable CDP topology discovery on the interface, use the **no** form of the command or the **topology neighbor disable** command.

> **topology neighbor cdp** [**proxy** *interface*]

> **no topology neighbor cdp** [**proxy** *interface*]

Syntax Description		
proxy *interface*	Specifies the interface capable of learning the topology to use as a proxy for CDP. Only OSC wave interfaces and ethernetdcc interfaces can be used as proxy interfaces.	

Defaults

Topology discovery is enabled on wdm interfaces when a valid proxy interface is available.

Topology discovery is disabled on tengigethernetphy interfaces.

For wdm interfaces, the OSC wave interface patched to the oscfilter interface on an OADM module is the default proxy interface.

For tengigethernetphy interfaces, the ethernetdcc interface on the same 10-GE transponder module is the default proxy interface.

Command Modes

Interface configuration

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
12.1(10)EV2	Support for tengigethernetphy interfaces was added.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines

CDP learns about the neighboring nodes the network topology. CDP is not supported on transparent interfaces. For this command to function properly, an OSC or ethernetdcc interface and CDP must be present and configured on the system.

> **Note** A tengigethernetphy interface can only use the ethernetdcc *slot*/*subslot*/**1** interface on the same 10-GE transponder module as its proxy.

You can use the **topology neighbor** command to statically add a wdm interface to the network topology, but you must first disable CDP on the interface. To configure a transparent interface as part of the network topology, use the **topology neighbor** command.

> **Note** You must correctly configure the patch connection between the mux/demux modules using the **patch** command. Otherwise, CDP cannot locate the wdm interfaces that connect to the trunk fiber and discover the topology neighbors.

> **Note** When a patch connection between a wdm interface on a module and a wdmrelay interface on a PSM is configured, topology learning on the wdm interface is disabled.

Examples   The following example shows how to enable CDP on a wdm interface.

```
Switch# configure terminal
Switch(config)# interface wdm 0/3
Switch(config-if)# topology neighbor cdp
```

Related Commands

Command	Description
patch	Configures the patch connections between the mux/demux modules.
show topology neighbor	Displays the topology configuration.
snmp-server enable traps topology	Enables SNMP trap notifications for the network topology.
topology neighbor	Adds a static entry for an interface to the network topology.
topology neighbor disable	Removes the interface from the network topology.

topology neighbor disable

To remove an interface from the network topology, use the **topology neighbor disable** command.

> **topology neighbor disable**

Syntax Description   This command has no other arguments or keywords.

Defaults   None

Command Modes   Interface configuration

Command History   This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.

SV-Release	Modification
12.2(18)SV	This command was integrated in this release.

S-Release	Modification
12.2(22)S	This command was integrated in this release.

Usage Guidelines   Use this command to remove an interface from the network topology, whether it was added with the **topology neighbor** command or the **topology neighbor cdp** command.

Examples   The following example shows how to remove an interface from the network topology.

```
Switch# configure terminal
Switch(config)# interface wdm 0/2
Switch(config-if)# topology neighbor disable
```

Related Commands

Command	Description
show topology neighbor	Displays the system connections.
topology neighbor	Adds a static entry for an interface to the network topology.
topology neighbor cdp	Enables CDP on the interface.

Cisco ONS 15540 ESPx Command Reference Guide

topology neighbor disable

INDEX

Cisco ONS 15540 ESPx Command Reference Guide