Cisco ONS 15540 ESP Troubleshooting Guide

Cisco IOS Release 12.2SV
February 2006

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

Text Part Number: OL-9654-01

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Cisco ONS 15540 ESP Troubleshooting Guide
© 2006 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface xi

Document Objectives xi

Audience xi

Document Organization xii

Related Documentation xii

Document Conventions xiii

Where to Find Safety and Warning Information xiv

Obtaining Documentation xiv

Cisco.com xiv

Product Documentation DVD xiv

Cisco Optical Networking Product Documentation CD-ROM xv

Ordering Documentation xv

Documentation Feedback xv

Cisco Product Security Overview xv

Reporting Security Problems in Cisco Products xvi

Obtaining Technical Assistance xvi

Cisco Technical Support & Documentation Website xvii

Submitting a Service Request xvii

Definitions of Service Request Severity xvii

Obtaining Additional Publications and Information xviii

CHAPTER 1

Troubleshooting Overview 1-1

General Model of Problem Solving 1-1

Maintaining Network Information 1-3

Initial Troubleshooting 1-3

Network and System Management 1-3

CiscoView 1-4

DFM 1-4

Third Party Troubleshooting Tools 1-4

Using General Diagnostic Commands 1-5

show Commands 1-5

debug Commands 1-6

ping Commands 1-7

traceroute Command 1-7
Online Diagnostics 1-7
Accessibility Test 1-8
OIR Test 1-8
Configuring Online Diagnostics 1-8
Displaying the Online Diagnostics Configuration and Results 1-9

CHAPTER 2 **Troubleshooting Network Connections 2-1**
Evaluating Component Connections and Configurations 2-1
Troubleshooting APS 2-2
Displaying APS Configuration 2-2
Debugging APS Configuration 2-4
Forcing a Manual Switchover 2-4
Determining Protection Schemes in Network Topologies 2-5
About OSC 2-5

CHAPTER 3 **Troubleshooting Client Side Interfaces 3-1**
Troubleshooting Client Side Transparent Interfaces 3-1
Determining Transparent Interface Connectivity 3-3
Using the debug Commands to Troubleshoot Client Side Interfaces 3-5

CHAPTER 4 **Troubleshooting Trunk Side Interfaces 4-1**
Troubleshooting Trunk Side Interfaces 4-1
Determining Trunk Side Connectivity 4-4
Troubleshooting OSCP Connections 4-5
Using the debug Commands to Troubleshoot Trunk Side Interfaces 4-7

CHAPTER 5 **Troubleshooting Network Topologies 5-1**
Checking Connectivity 5-1
Troubleshooting Unprotected Point-to-Point Topology 5-5
Troubleshooting Point-to-Point Topology with Splitter Protection 5-7
Troubleshooting Point-to-Point Topology with Line Card Protection 5-9
Troubleshooting Hubbed Ring Topology with Splitter Protection 5-11
Troubleshooting Hubbed Ring Topology with Line Card Protection 5-14
Troubleshooting Meshed Ring Topology with Splitter Protection 5-17
Troubleshooting Meshed Ring Topology with Line Card Protection 5-20

CHAPTER 6 **Troubleshooting the Cisco ONS 15540 Processor Card** 6-1

Verifying Processor Card Configuration 6-1

Recovering a Lost Password 6-4

Verifying NME Interface Configurations 6-5

Troubleshooting Processor Card Memory 6-7

Verifying Hardware and Software Versions 6-8

Verifying Hardware and Software Compatibility 6-10

Troubleshooting Redundant Processor Cards 6-13

Verifying Hardware and Software Versions of Redundant Processor Cards 6-13

Verifying Redundant Processor Card Functions 6-14

Checking the DDTs Database and Release Notes for Workarounds 6-17

Using Bug Navigator II 6-17

Checking Cisco IOS Release Notes 6-18

CHAPTER 7 **Troubleshooting Performance History Counter Problems** 7-1

7.1 Overview 7-1

7.2 Initial Troubleshooting Checklist 7-1

7.3 Interpreting Performance History Messages 7-2

7.4 Troubleshooting Performance History Counters 7-2

7.4.1 Some Counters Are Not Displayed 7-2

7.4.2 Performance History Counters Are Not Preserved Across CPU Switch Module Switchovers 7-3

Technical Support A-1

Gathering Information About Your Internetwork A-1

Getting the Data from Your System A-2

Providing Data to Customer Service A-2

INDEX

FIGURES

Figure 1-1 General Model of Problem Solving **1-2**

Figure 5-1 General Connection Troubleshooting Steps **5-2**

Figure 5-2 Point-to-Point Configuration Without Protection **5-5**

Figure 5-3 Point-to-Point Connection with Splitter Protection **5-7**

Figure 5-4 Point-to-Point Network with Line Card Protection **5-10**

Figure 5-5 Hubbed Ring Network with Splitter Protection **5-12**

Figure 5-6 Hubbed Ring Network with Line Card Protection **5-15**

Figure 5-7 Meshed Ring Network with Splitter Protection **5-18**

Figure 5-8 Meshed Ring Network with Line Card Protection **5-21**

Table 1-1 Useful Diagnostic Commands **1-6**

Table 2-1 Protection Schemes in Network Topologies **2-5**

Table 3-1 Signal Quality Fields and Errors in the Configuration **3-3**

Table 4-1 Signal Quality Fields and Errors in the Configuration **4-3**

Table 7-1 Some Counters Are Not Displayed **7-3**

Table 7-2 Performance History Counters Are Not Preserved Across CPU Switch Module Switchovers **7-3**

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
- 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 describes how to identify and resolve problems with your Cisco ONS 15540. 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

The *Cisco ONS 15540 ESP Troubleshooting Guide* is organized into the following chapters:

- Chapter 1, "Troubleshooting Overview," provides an overview of the troubleshooting features and functions.
- Chapter 2, "Troubleshooting Network Connections," provides troubleshooting information for connectivity and performance problems in optical network environments.
- Chapter 3, "Troubleshooting Client Side Interfaces," provides troubleshooting information for connectivity and performance problems in client side connections.
- Chapter 4, "Troubleshooting Trunk Side Interfaces," provides troubleshooting information for connectivity and performance problems in trunk side connections.
- Chapter 5, "Troubleshooting Network Topologies," provides troubleshooting information for point-to-point, ring, and meshed ring network topologies.
- Chapter 6, "Troubleshooting the Cisco ONS 15540 Processor Card," provides troubleshooting information for connectivity and performance problems in the processor card.
- Chapter 7, "Troubleshooting Performance History Counter Problems," describes the troubleshooting procedures used for performance history counter problems.
- Appendix A, "Technical Support," describes the process used to contact and provide your technical support representative with the information to resolve your problem.

Related Documentation

Use the *Cisco ONS 15540 ESP Troubleshooting Guide* in conjunction with the following referenced publications:

- *Cisco ONS 15540 ESP Planning Guide*

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

  Provides detailed information about installing the Cisco ONS 15540 ESP.
- *Cisco ONS 15540 ESP Configuration Guide*

  Provides detailed information about configuring the Cisco ONS 15540 ESP.
- *Cisco ONS 15540 ESP Command Reference*

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

  Describes the system alarms and error messages for the Cisco ONS 15540 ESP.
- *Network Management for the Cisco ONS 15540 ESP*

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

  Provides a full TL1 command and autonomous message set including parameters, AIDs, conditions and modifiers for the Cisco ONS 15540 ESP.
- *Regulatory Compliance and Safety Information for the Cisco ONS 15500 Series*

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

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

  Describes the Management Information Base (MIB) objects and explains how to access Cisco public MIBs for the Cisco ONS 15500 Series.
- *Cisco ONS 15540 ESP Software Upgrade Guide*

  Describes how to upgrade system images and functional images on the Cisco ONS 15540 ESP.
- *Introduction to DWDM Technology*

  Provides background information on the dense wavelength division multiplexing (DWDM) technology.
- *Cisco IOS Configuration Fundamentals Configuration Guide*

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

Document Conventions

This publication uses the following conventions:

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

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

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

Warning **IMPORTANT SAFETY INSTRUCTIONS**

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

SAVE THESE INSTRUCTIONS

Where to Find Safety and Warning Information

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

Obtaining Documentation

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

Cisco.com

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

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

Cisco Optical Networking Product Documentation CD-ROM

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

Ordering Documentation

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

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

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

Documentation Feedback

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

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

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

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

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

- For Nonemergencies—psirt@cisco.com

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

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

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

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

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

http://www.cisco.com/techsupport

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

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

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

Submitting a Service Request

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

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

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

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

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

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

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

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

  http://www.ciscopress.com

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

  http://www.cisco.com/packet

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

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

  or view the digital edition at this URL:

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

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

  http://www.cisco.com/ipj

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

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

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

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

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

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

Troubleshooting Overview

This chapter gives a brief overview of the various areas that might require troubleshooting. This chapter includes the following sections:

- General Model of Problem Solving, page 1-1
- Maintaining Network Information, page 1-3
- Initial Troubleshooting, page 1-3
- Network and System Management, page 1-3
- Third Party Troubleshooting Tools, page 1-4
- Using General Diagnostic Commands, page 1-5
- Online Diagnostics, page 1-7

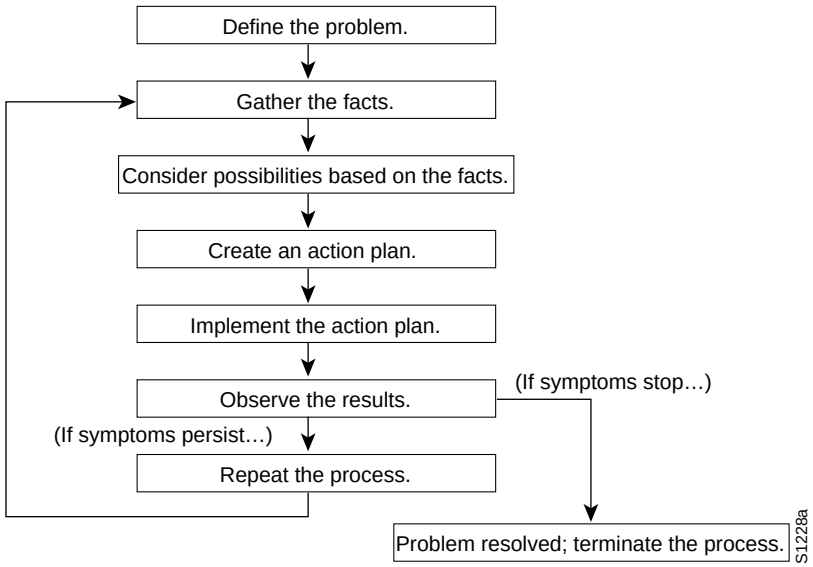
Basic troubleshooting processes, such as troubleshooting Ethernet connections, that are not specific to the Cisco ONS 15540 are not described in this document. This information is found online in other troubleshooting guides such as the *Cisco IOS Internetwork Troubleshooting Guide.*

General Model of Problem Solving

When troubleshooting a network environment, define the specific symptoms, identify all potential problems that could be causing the symptoms, and then systematically eliminate each potential problem (from most likely to least likely) until the symptoms disappear.

Figure 1-1 illustrates the general problem-solving model. This process is not a rigid outline for troubleshooting an internetwork. It is a foundation on which you can build a problem-solving process for your environment.

Figure 1-1 General Model of Problem Solving



The following steps detail the problem-solving process outlined in Figure 1-1:

Step 1 Analyze the network problem and create a clear problem statement. Define symptoms and potential causes.

Step 2 Gather the facts you need to help isolate possible causes.

Step 3 Consider possible causes based on the facts you gathered.

Step 4 Create an action plan based on those causes. Begin with the most likely problem and devise a plan in which you manipulate only *one* variable.

Step 5 Implement the action plan, performing each step carefully while testing to see whether the symptom disappears.

Step 6 Analyze the results to determine whether the problem is resolved.

Step 7 Terminate the process if the process is resolved.

Step 8 Create an action plan based on the next most probable cause on your list if the problem is not resolved. Return to Step 4 and repeat the process until the problem is solved.

Make sure that you undo anything you changed while implementing your action plan. Remember that you want to change only one variable at a time.

Note If you exhaust all the common causes and actions (either those outlined in this publication or others that you have identified in your environment), contact customer service. See Appendix A, "Technical Support," for additional information.

Maintaining Network Information

Maintaining the following details about your network helps with troubleshooting your system:

- Maintain an accurate physical and logical map of your internetwork that outlines the physical location of all of the devices on the network and how they are connected, as well as a logical map of network addresses, network numbers, and subnetworks.
- List all network protocols implemented in your network as well as a list of the network numbers, subnetworks, zones, and areas that are associated with them.
- Note which protocols are being routed and what the correct, up-to-date configuration information is for each protocol.
- Document all the points of contact to external networks, including any connections to the Internet. For each external network connection, note what routing protocol is being used.
- Document normal network behavior and performance so that you can compare current problems with a baseline.

Initial Troubleshooting

Before you start the troubleshooting process, confirm that the network and client connections were designed correctly using the information in the *Cisco ONS 15540 ESP Planning and Design Guide* and the interfaces were configured correctly using the information in the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

Next confirm the integrity of the hardware and its installation by performing the following:

- Reseat the cable.
- Clean the cable, connectors, couplers, and attenuators.
- Confirm that the Tx and Rx fiber optic connections are not mixed.
- Reseat the transponder modules and mux/demux modules to the optical backplane.
- Confirm all modules and motherboards are completely seated or the captive screws are tightened securely to completely mate the optical fiber connectors to the backplane.
- Check the signal level at each input and output to check for too much or too little attenuation.
- Verify that the mux/demux modules and transponder modules are in their proper slots.
- Verify that you are using the proper east and west mux/demux motherboard.

Network and System Management

This section describes the network management tools available for the Cisco ONS 15540. CiscoWorks 2000 supports a suit of network management applications of which the following are supported on the Cisco ONS 15540:

- CiscoView
- DFM (Device Fault Manager)

CiscoView

CiscoView is a device management application providing dynamic status, monitoring, and configuration information for a range of Cisco internetworking products including the Cisco ONS 15540. CiscoView displays a physical view of a device chassis, with color-coding of modules and ports for at-a-glance status. Monitoring capabilities display performance and other statistics. Configuration capabilities allow changes to devices if security privileges are granted.

Cisco ONS 15540 is supported by Embedded CiscoView and server based CiscoView. Online help for CiscoView is available for the server based CiscoView.

DFM

DFM reports faults that occur on Cisco devices, often identifying fault conditions before users of network services realize that the condition exists. DFM analysis technology differs from the traditional rules-based approach to event analysis. DFM analysis uses a top-down approach that starts by identifying the fault conditions that affect managed systems and are important to identify and analyze. Each fault condition causes a set of symptoms—a problem signature—that occurs within the faulty element and in related elements. DFM creates a causality mapping between the fault conditions and the symptoms. After the fault conditions and their symptoms are identified, this information is coded in the analysis model.

Because the event information necessary to diagnose fault conditions is present in the analysis model, DFM monitors only the events necessary to diagnose the condition. DFM simplifies event analysis: there are no rules to write and the analysis model guarantees that critical fault conditions are always identified.

DFM can operate as an independent management system or can integrate with existing management applications to add fault management to the functionality already in place.

For troubleshooting information relating to security implementations and information about configuring and using TACACS+, refer to the *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference*.

Third Party Troubleshooting Tools

In many situations, third-party troubleshooting tools can be helpful. For example, attaching an optical analyzer to a network is less intrusive than using the **debug** commands, which are processor intensive.

Here are some typical third-party tools used for troubleshooting internetworks:

- Optical cleaning kit—Keeps your optical cable connections clean. This should be in every tool kit that has anything to do with optical equipment. Several problems you encounter will typically be associated with dirty cables.
- Optical power meter—Measures the optical power coming from and going into a piece of equipment. This is the standard operating procedure for installing and troubleshooting optical equipment. Your optical power meter must be able to measure signals at 850 nm, 1310 nm, and 1550 nm.

Note Optical power meters need to be recalibrated once per year.

- TDR (time domain reflectometer)—Locates open circuits, short circuits, crimps, kinks, sharp bends, impedance mismatches, and other defects in metallic cables. A TDR reflects a signal off the end of the cable. Opens, shorts, and other problems reflect back the signal at different amplitudes, depending on the problem. A TDR measures the time it takes for the signal to reflect and calculates the distance to a fault in the cable. TDRs can also measure the length of a cable, and some TDRs can calculate the rate of propagation based on a configured cable length.
- OTDR (optical time domain reflector/reflectometer)—Checks end-to-end loss and detects fiber breaks, splice points in the optical fiber, and fiber attenuation. This tool is essential for initial network startup and later troubleshooting fiber breaks.
- BERT (bit error rate tester)—Tests OC-3, OC-12, and OC-48 ports for end connectivity of the wavelength if the client equipment is not yet available. BERT usually has a built-in power meter to test optical power of the circuit.
- Fiber microscope—Checks the fiber interface for dirt or anything else that could degrade the optical connection.
- Patch cables— Loops back the trunk side. You should keep an assortment of multimode and single-mode patch cables with you, including 1550 nm SM trunk side cables with MU-to-SC interfaces and SC-to-SC coupler. Use attenuators as needed.
- Fixed attenuators—Adds fixed attenuation levels to connections. Five attenuators with 5 dB at 1310 nm and five with 10 dB at 1310 nm, are a good start.
- Spectrum analyzer—Views the channel spectrum or analyzes light according to wavelength. It is useful when you suspect channel cross talk and for certifying equipment and performing periodic laser tests for stability.
- Network monitors—Tracks packets crossing a network, providing an accurate picture of network activity. Network monitors do not decode the contents of frames. They are useful for creating a baseline of normal performance. Monitors collect information such as packet sizes, the number of packets, error packets, overall usage of a connection, the number of hosts and their MAC addresses, and details about communications between hosts and other devices. This data can be used to create profiles of LAN traffic and assist in locating traffic overloads, planning for network expansion, detecting intruders, and distributing traffic more efficiently.

Using General Diagnostic Commands

You can use the **show**, **debug**, **ping**, and **traceroute** commands to monitor and troubleshoot your internetwork.

show Commands

You can use the **show** commands to perform many functions such as the following:

- Monitors the behavior of your Cisco ONS 15540 during initial installation
- Monitors normal network operation
- Isolates problem interfaces, nodes, media, or applications
- Determines when a network is congested
- Determines the status of servers, clients, or other neighbors

Table 1-1 lists some of the most commonly used **show** commands:

Table 1-1 Useful Diagnostic Commands

Command	Purpose
show interfaces **show interfaces fastethernet** **show interfaces thru** **show interfaces transparent** **show interfaces wave** **show interfaces wavepatch** **show interfaces wdm**	Displays statistics for the interfaces.
show controllers **show controllers ethernet** **show controllers** fastethernet	Displays statistics for processor interface controllers.
show running-config	Displays the currently running configuration.
show startup-config	Displays the configuration stored in NVRAM (nonvolatile RAM).
show flash	Displays the layout and content of Flash memory.
show buffers	Displays statistics for the buffer pools on the Cisco ONS 15540.
show memory	Shows statistics about the Cisco ONS 15540 memory, including free pool statistics.
show processes	Displays information about the active processes on the Cisco ONS 15540.
show stacks	Displays information about the stack utilization of processes and interrupt routines, and the reason for the last system reboot.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

For more information about **show** commands, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference* and the *Cisco IOS Configuration Fundamentals Command Reference* publication.

debug Commands

The **debug** privileged EXEC commands provide information about the traffic on (or *not* seen) on an interface, error messages generated by nodes on the network, protocol-specific diagnostic packets and cells, and other useful troubleshooting data.

Caution Be careful when using **debug** commands. Many of these commands are processor intensive and can cause serious network problems (such as degraded performance or loss of connectivity) if they are enabled on an already heavily loaded system. When you finish using a **debug** command, remember to disable it with its specific **no debug** command (or use the **no debug all** command to turn off all debugging).

In many situations, third-party diagnostic tools can be more useful and less intrusive than using **debug** commands. See the "Third Party Troubleshooting Tools" section on page 1-4.

ping Commands

To check host reachability and network connectivity, use the **ping** user EXEC or privileged EXEC command. This command can be used to confirm basic network connectivity on IP networks.

For IP, the **ping** command sends ICMP (Internet Control Message Protocol) echo messages. If a station receives an ICMP echo message, it sends an ICMP echo reply message back to the source.

Using the extended command mode of the **ping** privileged EXEC command, you can specify the supported IP header options, which allow the Cisco ONS 15540 to perform a more extensive range of test options. To enter **ping** extended command mode, enter the **ping** command at the command prompt followed by a return.

To see how the command works under normal conditions, use the **ping** command when the network is functioning properly. When you are troubleshooting, you can then see the difference between normal and abnormal operation.

For detailed information about using the **ping** and extended **ping** commands, refer to the *Cisco IOS Configuration Fundamentals Command Reference* publication.

traceroute Command

The **traceroute** user EXEC command discovers the routes packets follow when traveling to their destinations. With the **traceroute** privileged EXEC command, the supported IP header options are specified, and the Cisco ONS 15540 can perform a more extensive range of test options.

The **traceroute** command works by using the error message generated by a Cisco ONS 15540 when a datagram exceeds its TTL (Time-To-Live) value. First, probe datagrams are sent with a TTL value of one. This causes the first Cisco ONS 15540 to discard the probe datagrams and send back `time exceeded` error messages. The **traceroute** command then sends several probes, and displays the round-trip time for each. After every third probe, the TTL increases by one.

Each outgoing packet can result in one of two error messages. A `time exceeded` error message indicates that an intermediate Cisco ONS 15540 has seen and discarded the probe. A `port unreachable` error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet to an application. If the timer goes off before a response comes in, the **traceroute** command displays an asterisk (*).

The **traceroute** command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the **traceroute** command with the escape sequence.

To see how the command works under normal conditions, use the **traceroute** command when the network is functioning properly. When you are troubleshooting, you can then see the difference between normal and abnormal operation.

For detailed information about using the **traceroute** command, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*. For additional information on using **debug** commands refer to the *Cisco IOS Debug Command Reference.*

Online Diagnostics

This section describes the online diagnostics available for troubleshooting your Cisco ONS 15540. Online diagnostics provide the following types of tests:

- Accessibility tests between the processor and the modules.

- OIR (online insertion and removal) diagnostic tests.

The Cisco ONS 15540 displays an error message on the console when it detects a hardware failure or problem.

Note Online diagnostic tests only run on the active processor.

Accessibility Test

The accessibility tests ensure connectivity, at a configurable interval, between the following:

- Mux/demux modules
- Mux/demux motherboards
- Transponder modules
- Line card motherboards
- Active processor card
- Standby processor card, if it is present

OIR Test

OIR tests check the functioning of the processor and interfaces on a per-port basis. The processor performs these tests when the system boots up and when you insert a module or motherboard into a slot. The OIR test sends a packet to the interface loopback and expects to receive it within a certain time period. If the packet does not reach the port within the expected time period, or the received packet is corrupted, an error is registered and the port is changed to an administratively down state. Packets that are 1000 bytes in size are used in the test.

Configuring Online Diagnostics

To configure online diagnostics, use the following global configuration commands:

Command	Purpose
[**no**] **diag online**	Enables or disables online diagnostic tests on all components on the shelf.
[**no**] **diag online slot** *slot*	Enables or disables online diagnostic tests only on the components in a chassis slot.
[**no**] **debug diag online** [**background** | **online-insertion-removal** | **redundancy**]	Enables debugging of online diagnostic tests.

Examples

The following example shows how to enable all online diagnostic tests:

```
Switch# diag online
```

The following example shows how to enable online diagnostic tests for the components in slot 3:

```
Switch# diag online slot 3
```

The following example shows how to enable debugging for online diagnostics:

```
Switch# debug diag online
```

Displaying the Online Diagnostics Configuration and Results

To display the online diagnostics configuration and results, use the following EXEC command:

Command	Purpose
show diag online [**detail** | **slot** *slot*]	Displays information about the online diagnostic tests and the test results.

Example

The following example shows how to display detailed access test information:

```
Switch# show diag online
---------------------------------------------------
Online Diagnostics was DISABLED at 0 minutes
This information is the LAST status before disabling
---------------------------------------------------
Online Diagnostics Current Summary Information
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
On ACTIVE CPU card Slot: 6
CPU Uptime:    19 hours, 58 minutes

 Slot       CardType         Enabled     Bootup/     Periodic     Previous
                                        Insertion   Background   Failures
                                        tests       tests
 ~~~~~~   ~~~~~~~~~~~~~~     ~~~~~~~   ~~~~~~~~~   ~~~~~~~~~~    ~~~~~~~~
 0/*/*      Mx-DMx-Mthrbd       Yes      Pass          Pass           No

 1/*/*      Mx-DMx-Mthrbd       Yes      Pass          Pass           No

 2/*/*   XpndrMotherboard       Yes      Pass          Pass           No
 2/ 0/*  NPlugXpndrMonitor      Yes      Pass          Pass           No
 2/ 1/*  NPlugXpndrMonitor      Yes      Pass          Pass           No
 2/ 2/*  NPlugXpndrMonitor      Yes      Pass          Pass           No

 3/*/*   XpndrMotherboard       Yes      Pass          Pass           No
 3/ 0/*  NPlugXpndrMonitor      Yes      Pass          Pass           No
 3/ 1/*  NPlugXpndrMonitor      Yes      Pass          Pass           No
 3/ 2/*  NPlugXpndrMonitor      Yes      Pass          Pass           No
 3/ 3/*  NPlugXpndrMonitor      Yes      Pass          Pass           No

 4/*/*   XpndrMotherboard       Yes      Pass          Pass           No
 4/ 0/*  NPlugXpndrMonitor      Yes      Pass          Pass           No

 6/*/*         Queens CPU       Yes      Pass          Pass           No
```

Example

The following example shows how to display diagnostic test status and details:

```
Switch# show diag online details

Online Diagnostics Detailed Information
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
On ACTIVE CPU card Slot: 6
CPU Uptime:    19 hours, 58 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

Online Background Tests
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~    ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~   ~~~~~~~~~~~~
 0/*/*      Mx-DMx-Mthrbd    lrcAccess      Pass19 hours, 58        never
                           idpromAccess      Pass
_____________________________________________________________________________
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

Online Background Tests
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~    ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~   ~~~~~~~~~~~~
 1/*/*      Mx-DMx-Mthrbd    lrcAccess      Pass19 hours, 58        never
                           idpromAccess      Pass
_____________________________________________________________________________
Slot[2]:XpndrMotherboard
Enabled: Yes

Online Insertion Tests
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~    ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~   ~~~~~~~~~~~~
 2/*/*   XpndrMotherboard    lrcAccess      Pass    0 minutes       never
                           idpromAccess      Pass
 2/ 0/*  NPlugXpndrMonitor    scAccess      Pass    0 minutes       never
                            idpromAcces      Pass
 2/ 1/*  NPlugXpndrMonitor    scAccess      Pass    0 minutes       never
                            idpromAcces      Pass
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~    ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~   ~~~~~~~~~~~~
 2/ 2/*  NPlugXpndrMonitor    scAccess      Pass    0 minutes       never
                            idpromAcces      Pass

Online Background Tests
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~    ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~   ~~~~~~~~~~~~
 2/*/*   XpndrMotherboard    lrcAccess      Pass19 hours, 58        never
                           idpromAccess      Pass
 2/ 0/*  NPlugXpndrMonitor    scAccess      Pass19 hours, 58        never
                            idpromAcces      Pass
 2/ 1/*  NPlugXpndrMonitor    scAccess      Pass19 hours, 58        never
                            idpromAcces      Pass
 2/ 2/*  NPlugXpndrMonitor    scAccess      Pass19 hours, 58        never
                            idpromAcces      Pass
_____________________________________________________________________________
Slot[3]:XpndrMotherboard
Enabled: Yes

Online Insertion Tests
```

```
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~    ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~
 3/*/*   XpndrMotherboard    lrcAccess      Pass    0 minutes       never
                           idpromAccess     Pass
 3/ 0/*  NPlugXpndrMonitor    scAccess      Pass    0 minutes       never
                           idpromAcces      Pass
 3/ 1/*  NPlugXpndrMonitor    scAccess      Pass    5 minutes       never
                           idpromAcces      Pass
 3/ 2/*  NPlugXpndrMonitor    scAccess      Pass    0 minutes       never
                           idpromAcces      Pass
 3/ 3/*  NPlugXpndrMonitor    scAccess      Pass    0 minutes       never
                           idpromAcces      Pass

Online Background Tests
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~    ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~
 3/*/*   XpndrMotherboard    lrcAccess      Pass19 hours, 58        never
                           idpromAccess     Pass
 3/ 0/*  NPlugXpndrMonitor    scAccess      Pass19 hours, 58        never
                           idpromAcces      Pass
 3/ 1/*  NPlugXpndrMonitor    scAccess      Pass19 hours, 58        never
                           idpromAcces      Pass
 3/ 2/*  NPlugXpndrMonitor    scAccess      Pass19 hours, 58        never
                           idpromAcces      Pass
 3/ 3/*  NPlugXpndrMonitor    scAccess      Pass19 hours, 58        never
                           idpromAcces      Pass
_____________________________________________________________________________
Slot[4]:XpndrMotherboard
Enabled: Yes
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~    ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~

Online Insertion Tests
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~    ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~
 4/*/*   XpndrMotherboard    lrcAccess      Pass    0 minutes       never
                           idpromAccess     Pass
 4/ 0/*  NPlugXpndrMonitor    scAccess      Pass    0 minutes       never
                           idpromAcces      Pass

Online Background Tests
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~    ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~
 4/*/*   XpndrMotherboard    lrcAccess      Pass19 hours, 58        never
                           idpromAccess     Pass
 4/ 0/*  NPlugXpndrMonitor    scAccess      Pass19 hours, 58        never
                           idpromAcces      Pass
_____________________________________________________________________________
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
                           PCMCIAAccess     Pass

Online Background Tests
 Slot         CardType       TestType    Status   LastRunTime   LastFailTime
 ~~~~~~   ~~~~~~~~~~~~~~    ~~~~~~~~~    ~~~~~~   ~~~~~~~~~~~   ~~~~~~~~~~~~
 6/*/*         Queens CPU    srcStatus      Pass19 hours, 58        never
                             PCIAccess      Pass
                           PCMCIAAccess     Pass
```

CHAPTER 2

Troubleshooting Network Connections

This chapter provides troubleshooting information about connectivity of the physical interfaces in a network topology. This chapter includes:

- Evaluating Component Connections and Configurations, page 2-1
- Troubleshooting APS, page 2-2
- Determining Protection Schemes in Network Topologies, page 2-5
- About OSC, page 2-5

Evaluating Component Connections and Configurations

Evaluate your optical network by determining how the network components are connected and configured.

To display the overall configuration of the optical connections, use the following EXEC commands:

Command	Purpose
show aps	Displays the APS (Automatic Protection Switching) status for the entire system.
show connect {edges | intermediate [sort-channel | interface *slot/subcard/0*]}	Displays the connections through the shelf.

To familiarize yourself with the configuration of the optical network prior to troubleshooting, use the following commands:

Step 1 Use the **show aps** command to display the configuration of APS and the status of the connections involved.

```
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
~~~~~~~~~~~~~~~~~ ~~ ~~ ~~ ~~~ ~~~~~~~~~~~~~~~~ ~~~~~~~~~~~~~~~~~~~
```

```
Wavepatch10/0/0   Wk St Dn     Wavepatch10/0/1   Wavepatch10/0/0
Wavepatch10/1/0   Wk St Up     Wavepatch10/1/1   Wavepatch10/1/0
Wavepatch10/2/0   Wk St Up     Wavepatch10/2/1   Wavepatch10/2/0
Wavepatch10/3/0   Wk St Up     Wavepatch10/3/1   Wavepatch10/3/0
Wavepatch10/0/1   Pr St Dn     Wavepatch10/0/0   Wavepatch10/0/0
Wavepatch10/1/1   Pr Ac Up LOL Wavepatch10/1/0   Wavepatch10/1/0
Wavepatch10/2/1   Pr Ac Up LOL Wavepatch10/2/0   Wavepatch10/2/0
Wavepatch10/3/1   Pr Ac Up LOL Wavepatch10/3/0   Wavepatch10/3/0
```

Step 2 Check the AR (APS Role). It shows the working and protection interfaces.

Step 3 Check the AS (APS State). It shows the active and standby interfaces.

Step 4 Check the IS (Interface State). It shows the status of the working and protection interfaces.

Step 5 Use the **show connect intermediate** command to display the connections configured from the mux/demux module through the system to the transponders.

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

Step 6 Use the **show connect edges** command to display the connections configured from the mux/demux module through the system to the transponders and the wavelength being used.

```
Switch# show connect edges
client/
client/
wave           wdm   channel
------------  -----  -------
Trans2/0/0     0/0      1
Trans2/1/0     0/0      2
Trans2/2/0     0/0      3
```

Troubleshooting APS

This section describes the troubleshooting processes for APS (Automatic Protection Switching). APS provides redundancy and protects against module failures and fiber cuts. For detailed APS configuration, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

Displaying APS Configuration

To troubleshoot the APS configuration on the processor card, use the following commands:

Command	Purpose
show aps	Displays summary APS status information for the entire system.
show aps group *group-name*	Displays detailed APS status information for a specific group.
show aps detail	Displays detailed APS configuration and status information for the entire system.
show aps interface {transparent ***slot*/*subslot*/*port*** **| wavepatch** ***slot*/*subslot*/*port*****}**	Displays the APS information for a specific interface.

Follow these steps to troubleshoot the APS configuration on the processor card:

Step 1 Use the **show aps** command to display the configuration of APS and the status connections involved. You can see the output of the **show aps** command in the "Evaluating Component Connections and Configurations" section on page 2-1.

Step 2 Use the **show aps interface wavepatch** command to display APS information for a wave interface connection.

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

APS Group alpha :

 architecture.: 1+1, remote prov: 1+1
 span.........: end-to-end (network side splitter)
 direction....: prov: uni, current: uni, remote prov: uni
 revertive....: no
 created......: 13 hours, 54 minutes
 aps state....: associated (enabled)
 request timer: holddown: 5000 ms, max: 15000 ms, count 2
 search-up int: min: 2 secs, max: 32 secs
 switched chan: 0
 channel  ( 0): Wavepatch8/0/0 (STANDBY - UP)
              : channel  request: no-request
              : transmit request: no-request
              : receive  request: do-not-revert
 channel  ( 1): Wavepatch8/0/1 (ACTIVE - UP)
              : channel  request: no-request
              : switchover count: 1
              : last  switchover: 13 hours, 54 minutes
```

Step 3 Use the **show aps group** command to display APS information for a group named alpha.

```
Switch# show aps group alpha

APS Group alpha :

  architecture.: 1+1, remote prov: 1+1
  span.........: end-to-end (network side splitter)
  direction....: prov: uni, current: uni, remote prov: uni
  revertive....: no
  created......: 13 hours, 56 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): Wavepatch2/0/1 (STANDBY - UP)
```

```
                : channel  request: no-request
                : transmit request: no-request
                : receive  request: do-not-revert
channel  ( 1): Wavepatch2/0/0 (ACTIVE - UP)
                : channel  request: no-request
                : switchover count: 0
                : last  switchover: never
```

If you determine that APS is not configured correctly, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

Debugging APS Configuration

The debug privileged EXEC commands can provide a wealth of information about the status of APS.

Caution Exercise care when using **debug** commands. Many of these commands are processor intensive and can cause serious network problems (such as degraded performance or loss of connectivity) if they are enabled on an already heavily loaded Cisco ONS 15540. When you finish using a **debug** command, remember to disable it with its specific **no debug** command (or use the **no debug all** command to turn off all debugging).

To isolate problems and troubleshoot APS configuration on the Cisco ONS 15540, use the following **debug** commands in privileged EXEC mode. Use the **no** form of these commands to disable debugging.

Command	Purpose
debug aps	Starts debugging aps.

If you determine that APS is not configured correctly, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

Forcing a Manual Switchover

A manual switchover from working to protection fiber can be done in cases where upgrading or servicing is being performed, or in cases where an automatic switchover has occurred.

In the case of splitter protection, once the cause of the problem has been corrected, the system does not automatically revert to using the original working signal. The switchover to the formerly failed signal must be done manually. This might be desirable if the link originally configured as working was preferred because of its link loss characteristics or because of its distance advantage. Some protocols, such as ESCON, can experience lower data throughput at increasing distances, so you may want to move the working signal back to the shorter path.

Refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference* for instructions on forcing a manual switchover.

Determining Protection Schemes in Network Topologies

Table 2-1 outlines the protection schemes used in the different network topologies. For details on the protection schemes, refer to the *Cisco ONS 15540 ESP Configuration and Command Reference.* For details on network topologies, refer to the *Cisco ONS 15540 ESP Planning Guide*.

Table 2-1 Protection Schemes in Network Topologies

Topology	Without Protection	With Protection
Point-to-point	See the "Troubleshooting Unprotected Point-to-Point Topology" section on page 5-5.	See the "Troubleshooting Point-to-Point Topology with Splitter Protection" section on page 5-7. See the "Troubleshooting Point-to-Point Topology with Line Card Protection" section on page 5-9.
Hubbed Ring	NA	See the "Troubleshooting Hubbed Ring Topology with Splitter Protection" section on page 5-11. See the "Troubleshooting Hubbed Ring Topology with Line Card Protection" section on page 5-14.
Meshed Ring	NA	See the "Troubleshooting Meshed Ring Topology with Splitter Protection" section on page 5-17. See the "Troubleshooting Meshed Ring Topology with Line Card Protection" section on page 5-20.

About OSC

The Cisco ONS 15540 supports an optional out-of-band management channel for communicating between systems on the network. Using a 33rd wavelength (channel 0), the OSC (optical supervisory channel) allows control and management traffic to be carried without the necessity of a separate Ethernet connection to each Cisco ONS 15540 in the network. The OSC always terminates on a neighboring node. By contrast, data channels may or may not be terminated on a given node, depending on whether channels on the mux/demux modules are treated as express (pass-through) channels or add/drop.

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

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

For more information about the OSC and managing the Cisco ONS 15540, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

CHAPTER 3

Troubleshooting Client Side Interfaces

This chapter provides troubleshooting information on connectivity and performance problems in the client side interfaces of the Cisco ONS 15540.

This chapter includes the following sections:

- Troubleshooting Client Side Transparent Interfaces, page 3-1
- Determining Transparent Interface Connectivity, page 3-3
- Using the debug Commands to Troubleshoot Client Side Interfaces, page 3-5

Note For a description of the transponder modules, slot assignments, and detailed cabling information, refer to the *Cisco ONS 15540 ESP Hardware Installation Guide.*
For default configuration of the various modules, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference.*

Troubleshooting Client Side Transparent Interfaces

This section outlines the steps for performing basic interface checks and for verifying that a client side interface is enabled and functioning correctly.

Use the following command to check the optical interface configuration:

Command	Purpose
show interfaces transparent *slot/subcard/0*	Displays the status of the physical interface.

Follow these steps to troubleshoot the transparent interface connections:

Step 1 Use the **show interfaces transparent** *slot/subcard/0* command to display the configuration of a transparent interface:

```
Switch# show interfaces transparent 2/0/0
➔ Transparent2/0/0 is up, line protocol is up
    Encapsulation: GigabitEthernet
    Signal monitoring: on
    Time of last "monitor" state change 14:01:43
    Time of last "encapsulation" change 14:01:43
    Forward laser control: Off
```

```
Configured threshold Group: None
Code violation and running disparity error count(cvrd): 0
Number of times SF threshold exceeded: 0
Number of times SD threshold exceeded: 0
Loopback not set
Last clearing of "show interface" counters 14:01:43
Hardware is transparent
```

Step 2 Check for the following, if the interface is down:

- Confirm the integrity of the hardware and its installation. See the "Initial Troubleshooting" section on page 1-3. In case of hardware failure, swap the hardware. Refer to the *Cisco ONS 15540 ESP Hardware Installation Guide* for hardware information.

Note Just because the connector fits does not mean the cable is connected correctly or that the cable is the correct type.

- Check the status of the LEDs on the line card motherboards and the transponder modules.
- Make sure that the interfaces on both sides of the cables are enabled and in no-shutdown mode.
- Check the configuration of the interfaces (for example, check the framing, line coding, and scrambling).
- Ensure that the interfaces at both ends of the cable match.

Step 3 Use the **no shutdown** interface configuration command to reenable the interface, if the interface is administratively down.

If the interface continues to be down, check additional fields in the display to help you troubleshoot the connection.

```
Switch# show interfaces transparent 10/1/0
Transparent2/1/0 is down, line protocol is down
  Encapsulation: GigabitEthernet
  Signal monitoring: on
  Time of last "monitor" state change 14:04:26
  Time of last "encapsulation" change 14:04:26
  Forward laser control: Off
  Configured threshold Group: None
  Code violation and running disparity error count(cvrd): 0
  Number of times SF threshold exceeded: 0
  Number of times SD threshold exceeded: 0
  Loopback not set
  Last clearing of "show interface" counters 14:04:26
  Hardware is transparent
```

Note Not all of the fields listed in the steps may appear in every display and are dependent on the interface configuration and status.

If the interface is failing, check the configuration fields and errors that appear in the display. See Table 3-1.

Table 3-1 Signal Quality Fields and Errors in the Configuration

Configuration Fields and Errors	Indication
Signal quality:	
• LOL (Loss of light)	Attenuation or absence of signal as it propagates through the fiber.
• LOS (Loss of signal)	Attenuation or decay of signal strength as it propagates through the fiber.
Encapsulation field	Encapsulation field should match the actual interface on the client side.
Transmit and receive side errors: • Line code error count • Loss of sync error count • Clock count	Errors on the transmit side.
Encapsulation field errors:	
• Ingress line code error count	A loss of packet delineation.
• Ingress loss-of-sync error count	An optical module has lost clock synchronization.
• Ingress SONET BIP-1 error count	The bit interleaved parity error report calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B1 byte of the following frame. Differences indicate that section level bit errors have occurred. To check if the BIP-1 value is incrementing, check the BIP-1 value, wait a few seconds, and redisplay the transparent interface. If there are interleave parity errors, the number increments.
• Ingress SONET OOF error count	OOF (out of frame) error.
• Ingress SONET SEF error count	SEF (severely errored frame) count.
• Ingress clock count	Alarms associated with the primary or secondary clock source.

If you determine that the interface is configured incorrectly, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

Determining Transparent Interface Connectivity

To check transparent interface reachability to the mux/demux module and network connectivity, use the following commands:

Command	Purpose
show connect [edges | intermediate]	Displays the interface cross-connect configuration.
show topology	Displays the remote network connections.

Follow these steps to check the connectivity of a transparent interface through the system:

Step 1 Use the privileged EXEC **show connect intermediate** command to display the cross connection configuration for all interfaces or a single interface.

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

Switch#
```

Note The asterisk (*) next to the wavepatch interface number indicates the active wavepatch interface in the receive direction on the splitter protected line card motherboard.

```
Switch# show connect intermediate interface transparent 10/0/0
Client      : Transparent10/0/0
Wave        : Wave10/0
Wavepatch   : Wavepatch10/0/0 (active)  Wavepatch   : Wavepatch10/0/1
Filter      : Filter0/3/0               Filter      : Filter1/3/0
Wdm         : Wdm0/3                    Wdm         : Wdm1/3
Thru        : Thru0/0                   Thru        : Thru1/0
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 (trunk) : Wdm0/2                    Wdm         : Wdm1/2
Switch#
```

Step 2 Use the privileged EXEC **show connect edge** command to display the edge interface connections for all interfaces.

```
Switch# show connect edges
client/
wave          wdm  channel
------------  ---  -------
Trans10/0/0   0/3    25
Trans10/1/0   0/3    26
Trans10/2/0   0/3    27
Trans10/3/0   0/3    28
```

Step 3 Use the **show topology** command to display the connections to the neighbor nodes.

```
Switch# show topology

Physical Topology:

Local Port   Neighbor Node       Neighbor Port
----------   -------------       -------------
 2            Node2               wdm0/0
 4            Node4               wdm1/1
```

To continue troubleshooting the trunk side connections, see Chapter 2, "Troubleshooting Network Connections" and Chapter 4, "Troubleshooting Trunk Side Interfaces."

If you determine that the interface is configured incorrectly, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

Using the debug Commands to Troubleshoot Client Side Interfaces

The debug privileged EXEC commands can provide a wealth of information about the traffic being seen (or *not* seen) on an interface.

Caution Exercise care when using **debug** commands. Many of these commands are processor intensive and can cause serious network problems (such as degraded performance or loss of connectivity) if they are enabled on an already heavily loaded system. When you finish using a **debug** command, remember to disable it with its specific **no debug** command (or use the **no debug all** command to turn off all debugging).

To isolate problems and troubleshoot the client side interfaces of the Cisco ONS 15540, use the following **debug** commands in privileged EXEC mode. Use the **no** form of these commands to disable debugging.

Command	Purpose
debug aps	Starts debugging APS[1] operation.
debug cdp	Starts debugging CDP[2] information.
debug lcmdc	Starts debugging optical LC/MDC[3].
debug ports	Starts debugging port connections.
debug oscp	Starts debugging OSCP[4].

1. APS = Automatic Protection Switching
2. CDP = Cisco Discovery Protocol
3. LC/MDC = line card/mux-demux card
4. OSCP = Optical Supervisory Channel Protocol

If you determine that the connection is configured incorrectly, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

CHAPTER 4

Troubleshooting Trunk Side Interfaces

This chapter provides troubleshooting information on connectivity and performance problems in the trunk side interfaces of the Cisco ONS 15540.

This chapter includes the following sections:

- Troubleshooting Trunk Side Interfaces, page 4-1
- Determining Trunk Side Connectivity, page 4-4
- Troubleshooting OSCP Connections, page 4-5
- Using the debug Commands to Troubleshoot Trunk Side Interfaces, page 4-7

Note For a description of the mux/demux motherboards and modules, slot assignments, and detailed cabling information, refer to the *Cisco ONS 15540 ESP Hardware Installation Guide.* For information on configuration and protection modes, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

Troubleshooting Trunk Side Interfaces

This section outlines the steps for performing basic interface checks and for verifying that a trunk side interface is enabled and functioning correctly.

Use the following commands to display the status and configuration of the trunk side interfaces:

Command	Purpose
show interfaces wave *slot/subcard*	Displays the status and configuration of the wave interface on the transponder module.
show interfaces wavepatch *slot/subcard/port*	Displays the status and configuration of the wavepatch interface.
show interfaces thru *slot/subcard*	Displays the status and configuration of the thru interface.

Command	Purpose
show interfaces wdm *slot/subcard*	Displays the status and configuration of the wdm interface.
show interfaces wave {**0** | **1**}	Displays the status and configuration of the OSC wave interface on the mux/demux motherboard.

Follow these steps to check the status and configuration of the trunk side interface:

Step 1 Use the **show interfaces wave** *slot/subcard* command to display information about a specific wavelength generated by a transponder module. This is the most useful trunk side interface troubleshooting command. The **show interfaces wave** *slot/subcard* command displays the status of the entire connection from the optical backplane side of the transponder module to the next DWDM node interface connection. If this command indicates the connection is up, the connection is up the entire length of the connection to the next node. If this connection is down, then use the subsequent commands to confirm the individual connections across the system.

```
Switch# show interfaces wave 5/0
Wave5/0 is up, line protocol is up
  Channel: 13   Frequency: 193.6 Thz    Wavelength: 1548.51 nm
  Active Wavepatch : Wavepatch5/0/0
  Splitter Protected: No
➔ Receiver power level: -17.68 dBm
  Forward laser control: Off
  Laser safety control: Off
  Osc physical port: No
  Wavelength used for inband management: No
  Configured threshold Group: None
  Code violation and running disparity error count(cvrd): 0
  Number of times SF threshold exceeded: 0
  Number of times SD threshold exceeded: 0
  Loopback not set
  Last clearing of "show interface" counters 14:12:36
  Hardware is data_only_port
Switch#
```

Step 2 Check for the following if the interface is down:

- Confirm the integrity of the hardware and its installation. See the "Initial Troubleshooting" section on page 1-3. In case of hardware failure, swap the hardware.
- Ensure that the proper type of cables have been installed correctly. Refer to the cabling information in the *Cisco ONS 15540 ESP Hardware Installation Guide*.

  Note Just because the connector fits does not mean the cable is connected correctly or that the cable is the correct type.

- Check the status of the LEDs on the mux/demux motherboards and the mux/demux modules.
- Make sure that the interfaces on both sides of the cables are enabled and in no-shutdown mode.
- Check the configuration of the interfaces (for example check the framing, line coding, and scrambling).
- Ensure that the interfaces at both ends of the cable match.

Step 3 Use the **no shutdown** interface configuration command to reenable the interface if the interface is administratively down.

Step 4 Check additional fields in the display to help you troubleshoot the connection if the interface continues to be down. See Table 4-1.

Table 4-1 Signal Quality Fields and Errors in the Configuration

Configuration Fields and Errors	Indication
Receive power level	Power level at the connection to within +/- 1 dBm. Check the power levels and attenuation.
Signal quality:	
• LOS (loss of signal)	Attenuation or absence of signal as it propagates through the fiber.
• LOL (loss of lock)	Attenuation or decay of signal strength as it propagates through the fiber.
• Good	Acceptable signal levels.
BIP-1 field	The bit interleaved parity error report calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B1 byte of the following frame. Differences indicate that section level bit errors have occurred. To check if the BIP-1 value is incrementing, note the BIP-1 value, wait a few seconds, redisplay the wave interface. If there are interleave parity errors, the BIP-1 count increments

Step 5 Use the **show interfaces wavepatch** command to display information about the receive light path on the transponder motherboard.

```
Switch# show interface Wavepatch10/0/0
Wavepatch10/0/0 is up, line protocol is up
  Hardware is passive_port
Switch#
```

Step 6 Check the Wavepatch field to see if the connection across the backplane is up.

Step 7 Use the **show interfaces thru** command to display information about the thru interface to the next mux/demux module.

```
Switch# show interfaces thru 0/1
Thru0/1 is up, line protocol is up
 Patched Interface: Wdm0/2
  Hardware is thru_port
Switch#
```

Step 8 Check the Thru field to see if the interface is up. This interface should never be down.

Step 9 Use the **show interfaces wdm** command to display information about the wdm interface to the neighbor node.

```
Switch# show interfaces wdm 0/1
Wdm0/1 is up, line protocol is up
 Patched Interface: Thru0/0
 Wdm Hw capability: N/A
 Num of Wavelengths Add/Dropped: 8
 List of Wavelengths: 9, 10, 11, 12, 13, 14, 15, 16
  Hardware is wavelength_add_drop
```

```
Switch#
```

Step 10 Check the Wdm field to see if the interface is up.

Step 11 Check the line protocol field to see if the status is up.

Step 12 Use the **show interfaces wave 0 or 1** command to display information about the OSC interface on the mux/demux motherboard to the OSC connection on the mux/demux module.

```
Switch# show interfaces wave 0
Wave0 is up, line protocol is up
  Channel: 0    Frequency: 191.9 Thz    Wavelength: 1562.24 nm
  Signal quality: Good
  Laser safety control: Off
  Osc physical port: Yes
  Wavelength used for inband management: No
  Configured threshold Group: None
  CDL HEC error count: 0
  Number of times SF threshold exceeded: 0
  Number of times SD threshold exceeded: 0
  Last clearing of "show interface" counters never
  Hardware is OSC_phy_port
  Interface is unnumbered. Using address of Loopback1 (1.1.1.2)
  MTU 1492 bytes, BW 10000000 Kbit, DLY 0 usec,
     reliability 0/255, txload 1/255, rxload 1/255
  Encapsulation SNAP, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
Switch#
```

Step 13 Check the Wave field to see if the interface is up.

Step 14 Check the line protocol field to see if the status is up.

Note In Steps 5 to 14, if the interface is down where the line protocol software process might have determined that the line is unusable, go through the items listed in Step 2. If you determine that the connection is configured incorrectly, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

Determining Trunk Side Connectivity

To check trunk side connectivity in the network, use the **show connect** command.

Command	Purpose
show connect [edges | intermediate]	Displays the interface cross connection configuration.

Follow these steps to check the connectivity of a trunk side interface through the system:

Step 1 Use the EXEC **show connect** command to display the interface cross connection configuration:

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

Step 2 Use the EXEC **show connect edges** command to display the edge interface connections for all interfaces:

```
Switch# show connect edges
client/
wave          wdm  channel
------------  ---  -------
Trans10/0/0   0/3    25
Trans10/1/0   0/3    26
Trans10/2/0   0/3    27
Trans10/3/0   0/3    28
```

If you determine that the connection is configured incorrectly, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

Troubleshooting OSCP Connections

The OSCP (Optical Supervisory Channel Protocol) Hello protocol is used between the OSC wave interface on the Cisco ONS 15540 and the OSC wave interface on the next connected node. Use the following commands to display the status and configuration of the OSCP connections:

Command	Purpose
show oscp info	Displays the status and configuration of the OSCP for the switch.
show oscp interface	Displays the status and configuration of the local and remote interfaces running the OSCP.
show oscp neighbor	Displays information about the identity of the neighbors communicating with the system through the OSCP.
show oscp statistics [**wave** *slot*]	Displays OSCP Hello statistics for an OSC interface.
show oscp traffic [**wave** *slot*]	Displays OSCP control traffic for an OSC interface.

Use the following steps to check the status and configuration of the OSCP connection:

Step 1 Use the **show oscp info** command to display information about the OSCP configuration.

```
Switch# show oscp info

OSCP protocol version 1, Node ID        0202.0304.0506
No. of interfaces 0, No. of neighbors 0
Hello interval 50 tenth of sec, inactivity factor 5,

Hello hold-down 1 tenth of sec
Supported OSCP versions:newest 1, oldest 1
```

Step 2 Use the **show oscp interface** command for status information for the local and remote interfaces running OSCP.

```
Switch# show oscp interface

OSC Interface(s)
Local Port    Port ID  Status  OSC St  Rem Port ID Rem Node Id
~~~~~~~~~~~~~ ~~~~~~~  ~~~~~~  ~~~~~~  ~~~~~~~~~~~ ~~~~~~~~~~~~~~
wave0         1010000  Active    2way   1010000    0061.3a7b.4b00
wave1         0010000  Active    2way   0010000    0061.3a7b.4b01
```

Step 3 Use the **show osp neighbor** command to display information on the identity of the neighbors communicating with the system through the OSC.

```
Switch# show oscp neighbor

OSC Neighbor(s)

Neighbor Node Id:0061.3a7b.4b00
Port list:
Local Port    Port ID  Rem Port ID OSC state
~~~~~~~~~~~~~ ~~~~~~~~ ~~~~~~~~~~~ ~~~~~~~~~
wave0         1010000    1010000        2way
wave1         0010000    0010000        2way
```

Step 4 Use the **show oscp statistics** command to the display OSCP statistics, which can be used to debug OSCP.

```
Switch# show oscp statistics hello wave 1

OSC Hello Statistics:

int wave1

Event                 Count
~~~~~~~~~~~~           ~~~~~~~~~
hold down              2
Hello Tx               345
Hello Rx               347
Hello discards         0
OSC go down            0
```

Step 5 Use the **show oscp traffic** command to display OSCP control traffic statistics, which show the count of different protocol packets that were transmitted over the OSC channel.

```
Switch# show oscp traffic
OSC Traffic Statistics:

interface Wave1
Description         Count
~~~~~~~~~~~~    ~~~~~~~~~
Tx IP pkt           0
```

```
Rx IP pkt           0
Tx CDP pkt          0
Rx CDP pkt          0
Tx OSCP pkt         0
Rx OSCP pkt         0
Rx pkt dropped      0

Switch#
```

If you determine that the connection is configured incorrectly, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

Using the debug Commands to Troubleshoot Trunk Side Interfaces

The debug privileged EXEC commands can provide a wealth of information about the traffic being seen (or *not* seen) on an interface.

Caution Exercise care when using **debug** commands. Many of these commands are processor intensive and can cause serious network problems (such as degraded performance or loss of connectivity) if they are enabled on an already heavily loaded Cisco ONS 15540. When you finish using a **debug** command, remember to disable it with its specific **no debug** command (or use the **no debug all** command to turn off all debugging).

To isolate problems and troubleshoot the client side fiber optic connections of the Cisco ONS 15540, use the following **debug** commands in privileged EXEC mode. Use the **no** form of these commands to disable debugging.

Command	Purpose
debug ports {**errors** | **events**} **wave** ***number***	Starts debugging the wave interface.
debug ports {**errors** | **events**} **wdm** *slot/subcard/0*	Starts debugging the wdm interface.

If you determine that the connection is configured incorrectly, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

CHAPTER 5

Troubleshooting Network Topologies

This chapter provides information on troubleshooting point-to-point, ring, and meshed ring network topologies. This chapter includes the following sections:

- Checking Connectivity, page 5-1
- Troubleshooting Unprotected Point-to-Point Topology, page 5-5
- Troubleshooting Point-to-Point Topology with Splitter Protection, page 5-7
- Troubleshooting Point-to-Point Topology with Line Card Protection, page 5-9
- Troubleshooting Hubbed Ring Topology with Splitter Protection, page 5-11
- Troubleshooting Hubbed Ring Topology with Line Card Protection, page 5-14
- Troubleshooting Meshed Ring Topology with Splitter Protection, page 5-17
- Troubleshooting Meshed Ring Topology with Line Card Protection, page 5-20

Each of these topologies can be configured with or without protection. For detailed information on network topologies, refer to the *Cisco ONS 15540 ESP Planning Guide* and for information on how to configure these topologies, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

Checking Connectivity

There are two procedures for troubleshooting connections in network topologies. The first involves checking the connectivity of the interfaces. If that fails, then the second involves running the more disruptive loopback tests.

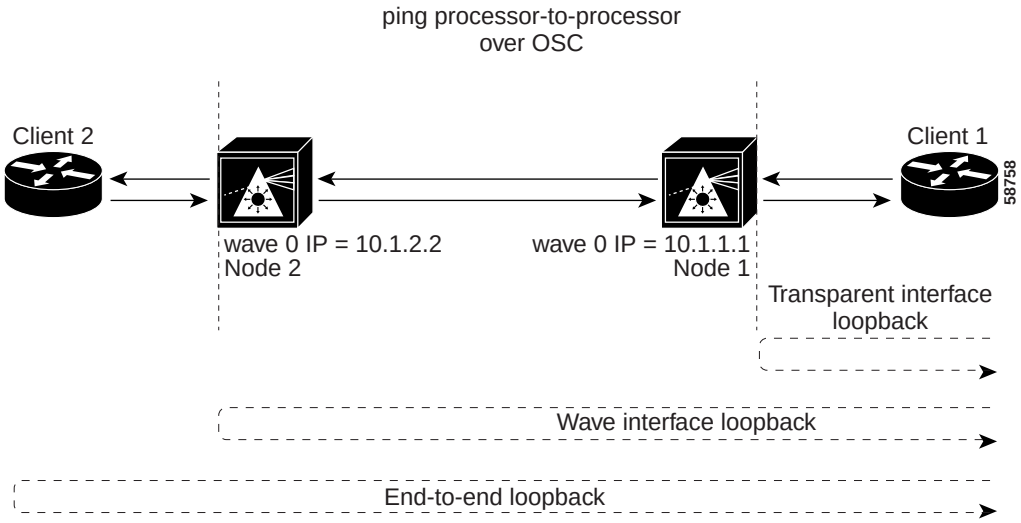
Loopback tests are an important part of troubleshooting. They are used to isolate the fault on an end-to-end circuit (especially when the circuit is down). The **loopback** diagnostic command causes traffic going out of a transparent or a wave interface to come back to the system and confirms the connection.

Caution When you configure loopback on an interface, communication over the link is interrupted but performance statistics are still updated.

Figure 5-1 shows a simple, point-to-point topology without protection between two Cisco ONS 15540 systems, node 1 and node 2. Some steps may seem redundant but following this process in this order should help troubleshoot the connection with the least disruption to the other connections on the network.

Note The following troubleshooting process assumes that the OSC wave interfaces are configured between the Cisco ONS 15540 systems. Without the OSC configured, troubleshooting the Cisco ONS 15540 connections requires you to log into each system and confirm each individual transparent and wave interface individually.

Figure 5-1 General Connection Troubleshooting Steps



To troubleshoot the configuration and status of the optical connections, use the following EXEC commands:

Command	Purpose
show interfaces transparent *slot/subcard/0*	Shows the status of the physical interfaces between the Cisco ONS 15540 and the clients.
show interfaces wave *slot/subcard*	Displays the status and configuration of the wave interface between Cisco ONS 15540 systems.
ping {*ip-address* | *hostname*}	Confirms the connection between OSC wave interfaces and the system fiber connections.
[**no**] **loopback**	Enables and disables loopback on the interface.

Follow these general steps to troubleshoot an optical fiber network connection between two end user clients:

Step 1 From node 1, use the **show interfaces transparent** command to display the connection between the transparent interface on the Cisco ONS 15540 and the client equipment.

```
Node1# show interfaces transparent 2/2/0
Transparent2/2/0 is up, line protocol is up
  Encap: Sonet    Rate: oc12
  Signal monitoring: on
  Configured threshold Group: None
  Threshold monitored for: BIP1 error
```

```
  Set threshold SF:10e-5  SD:10e-7
  Bip1 Count: 0
  Number of times SF threshold exceeded: 0
  Number of times SD threshold exceeded: 0
  Number of errored seconds: 0
  Number of severely errored seconds: 0
  Number of severely errored framing seconds: 0
  Number of times SEF alarm raised: 0
  Hardware is transparent
  Encapsulation UNKNOWN, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 04:17:45
Node1#
```

The **show interfaces transparent** command indicates whether the connection between the Cisco ONS 15540 and the client equipment is up. See the "Troubleshooting Client Side Transparent Interfaces" section on page 3-1 for information about the fields in this display.

Step 2 From node 1, use the **show interfaces wave** command to display the status of the trunk side laser on the transponder.

```
Node1# show interfaces wave 2/2
➔ Wave2/2 is up, line protocol is up
  Channel: 3    Frequency: 192.3 Thz    Wavelength: 1558.98 nm
  Active Wavepatch : Wavepatch2/2/0
  Splitter Protected: No
  Receiver power level: -15.34 dBm
  Forward laser control: Off
  Laser safety control: Off
  Osc physical port: No
  Wavelength used for inband management: No
  Configured threshold Group: None
  Code violation and running disparity error count(cvrd): 0
  Number of times SF threshold exceeded: 0
  Number of times SD threshold exceeded: 0
  Loopback not set
  Last clearing of "show interface" counters 14:35:39
  Hardware is data_only_port
Node1#
```

The **show interfaces wave** command indicates whether the connection between the Cisco ONS 15540 and the next neighboring node is up. See the Chapter 4, "Troubleshooting Trunk Side Interfaces," for information about the fields in this display.

Step 3 From node 1, use the **ping** command and the IP address of the node 2 wave 0 interface. The following **ping** command tests the connection between the processor on node 1, through the wave 0 interface, to the processor on node 2.

```
Node1# ping 10.1.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/72/76 ms
Node1#
```

The **ping** command between the nodes proves the trunk connection between node 1 and node 2 has not failed. It does not indicate if the individual channel connections have been misconfigured or one of the patch connections or components has failed.

For IP address configuration instructions for the OSC channel interface, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

If these three steps have not found the failed connection between nodes, continue with the following more disruptive connection loopback troubleshooting steps.

Caution The following troubleshooting steps for the individual channels and components of the Cisco ONS 15540 are disruptive to the client connections and can only be completed with login access to the client end-station equipment connected to the Cisco ONS 15540.

Step 4 From node 1, configure a loopback on the transparent interface that connects to the client equipment.

```
Node1(config)# interface transparent10/0/0
Node1(config-if)# loopback
Node1(config-if)# end
Node1#
```

Confirm the loopback configuration using the **show interfaces transparent** command.

```
Node1# show interfaces transparent10/0/0
→ Transparent10/0/0 is up, line protocol is up
    Encapsulation: GigabitEthernet
    Signal monitoring: on
    Time of last "monitor" state change 14:36:48
    Time of last "encapsulation" change 14:36:48
    Forward laser control: Off
    Configured threshold Group: None
    Code violation and running disparity error count(cvrd): 0
    Number of times SF threshold exceeded: 0
    Number of times SD threshold exceeded: 0
    Loopback set
    Last clearing of "show interface" counters 14:36:48
    Hardware is transparent
Node1#
```

Loopback should appear as set in the **show interfaces transparent** display.

From the client equipment connected to node 1, confirm the connection to the client appears as looped back. This proves the connection from the client to the transparent interface on node 1 is working.

Note Before continuing with the next loopback test, disable loopback on the transparent interface using the **no loopback** command.

Step 5 From node 2, configure the wave interface between the Cisco ONS 15540 and the far-end client loopback connection.

```
Node2(config)# interface wave10/0
Node2(config-if)# loopback
Node2(config-if)# end
Node2#
```

Confirm the loopback configuration using the **show interfaces wave** command.

```
Node2# show interfaces wave 10/0
Wave10/0 is up, line protocol is up
  Channel: 25   Frequency: 195.1 Thz    Wavelength: 1536.61 nm
  Active Wavepatch : Wavepatch10/0/0
  Splitter Protected: No
  Receiver power level: -6.0 dBm
  Forward laser control: Off
  Laser safety control: Off
  Osc physical port: No
  Wavelength used for inband management: No
```

```
  Configured threshold Group: None
➔ Loopback set
  Last clearing of "show interface" counters never
  Hardware is data_only_port
Node2#
```

Loopback should appear as set in the **show interfaces wave** display.

From the client connection through node 1 to node 2, confirm the connection to the client is looped back. This proves the connection from the client to the wave interface on node 2 is working.

From the client equipment connected to node 2, configure a loopback connection through the entire network end-to-end. This confirms the connection between the clients connected to node 1 and node 2 at both ends.

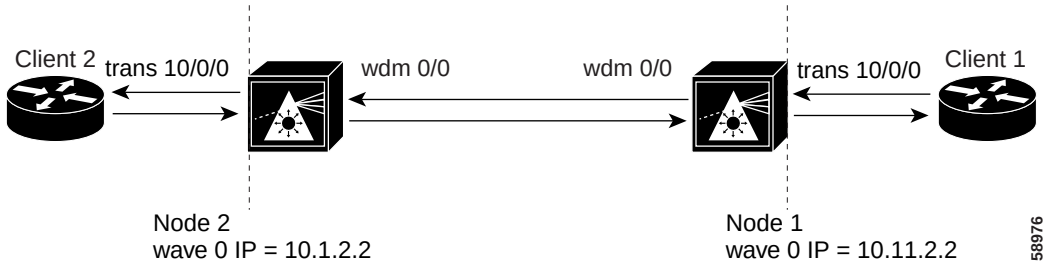
Troubleshooting Unprotected Point-to-Point Topology

Figure 5-2 shows an unprotected topology with two nodes. Both nodes use channels 1-32 and use the following:

- Transparent interfaces 2/0/0 through 11/3/0 on west line card motherboards
- Mux/demux module wdm 0/0 out to the west

To troubleshoot a point-to-point configuration with only user level protection, you must visually check for irregular connections and component LEDs, check for system alarms or error messages, use the trial-and-error method, or replace components until you solve the problem.

Figure 5-2 Point-to-Point Configuration Without Protection



For an example configuration of an unprotected point-to-point topology, see the *Cisco ONS 15540 ESP Planning Guide.*

To troubleshoot the configuration and status of point-to-point unprotected topology, use the following EXEC commands:

Command	Purpose
show interfaces transparent *slot/subcard/0*	Shows the status of the physical interfaces between the Cisco ONS 15540 and the clients.
show interfaces wave *slot/subcard*	Displays the status and configuration of the wave interface between Cisco ONS 15540 systems.

Command	Purpose
ping {*ip-address* | *hostname*}	Confirms the connection between OSC wave interfaces and the system fiber connections.
[**no**] **loopback**	Enables and disables loopback on the interface.

Use the following steps to troubleshoot a point-to-point unprotected topology between two end user clients:

Step 1 From node 1, use the **show interfaces transparent** command to display the connection between the transparent interface on the Cisco ONS 15540 and the client equipment.

The **show interfaces transparent** command indicates whether the connection between the Cisco ONS 15540 and the client equipment is up. See the "Troubleshooting Client Side Transparent Interfaces" section on page 3-1 for information about the fields in this display.

Step 2 From node 1, use the **show interfaces wave** command to display the connection status of the trunk side laser on the transponder.

The **show interfaces wave** command indicates whether the connection between the Cisco ONS 15540 and the neighboring node is up. See the Chapter 4, "Troubleshooting Trunk Side Interfaces," for information about the fields in this display.

Step 3 From node 1, use the **ping** command and the IP address of the node 2 wave 0 OSC interface. The following **ping** command tests the connection between the processor on node 1, through the OSC wave 0 interface, to the processor on node 2.

Using the **ping** command between the nodes over the OSC interface proves the connection between the two nodes has not failed. It does not prove that the individual channel connections have not been misconfigured or one of the patch connections or components has not failed.

For IP address configuration instructions for the OSC channel interface, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

If these three steps have not found the failed connection between the nodes, continue with the following more disruptive connection loopback troubleshooting steps.

Caution The following troubleshooting steps for the individual channels and components of the Cisco ONS 15540 are disruptive to the client connections and can only be completed with login access to the client end-station equipment connected to the Cisco ONS 15540.

Step 4 From node 1, configure the transparent interface connected to the client equipment as a loopback connection using the instructions in the "Checking Connectivity" section on page 5-1.

Confirm the loopback configuration using the **show interfaces transparent** command. Loopback should appear as set in the **show interfaces transparent** display.

From the client equipment connected to node 1, confirm the connection to the client appears as looped back. This proves the connection from the client to the transparent interface on node 1 is working.

Note Before continuing with the next loopback test, disable loopback on the transparent interface connected to the near end client.

Step 5 From node 2, configure the wave interface between the Cisco ONS 15540 and the far-end client loopback connection using the instructions in the "Checking Connectivity" section on page 5-1.

Confirm the loopback configuration using the **show interfaces wave** command. Loopback should appear as set in the **show interfaces wave** display.

From the client connection through node 1 to node 2, confirm the connection to the client is looped back. This proves the connection from the client to the wave interface on node 2 is working.

Step 6 From the client equipment connected to node 1, configure a loopback connection through the entire network end-to-end. This confirms the connection between the clients connected to node 1 and node 2 at both ends.

Troubleshooting Point-to-Point Topology with Splitter Protection

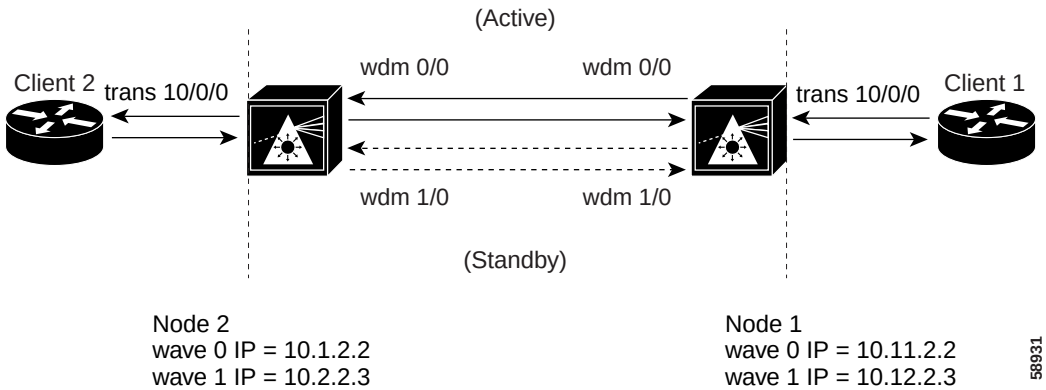
Figure 5-3 shows a splitter protected topology with two nodes. Both nodes use channels 1-32 and use the following:

- Transparent interfaces 2/0/0 through 11/3/0 on splitter protected line card motherboards
- Mux/demux module wdm 0/0 patched to wdm 0/0 out to the west
- Mux/demux module wdm 1/0 patched to wdm 1/0 out to the east

Note For splitter protected connections, alarms are only generated for the active side of the connection. Failures on the standby connection do not generate alarms.

For an example configuration of a splitter protected point-to-point topology, refer to the *Cisco ONS 15540 ESP Planning Guide.*

Figure 5-3 Point-to-Point Connection with Splitter Protection



To troubleshoot the configuration and status of the point-to-point connection with splitter protection, use the following EXEC commands:

Command	Purpose
show interfaces transparent *slot/subcard/0*	Shows the status of the physical interfaces between the Cisco ONS 15540 and the clients.
show interfaces wave *slot/subcard*	Displays the status and configuration of the wave interface between Cisco ONS 15540 systems.
ping {*ip-address* | *hostname*}	Confirms the connection between OSC wave interfaces and the system fiber connections.
[**no**] **loopback**	Enables and disables loopback on the interface.

Follow these general steps to troubleshoot an optical fiber network connection between two end user clients on a splitter protected point-to-point topology:

Step 1 From node 1, use the **show interfaces transparent** command to display the connection between the transparent interface on the Cisco ONS 15540 and the client equipment.

The **show interfaces transparent** command indicates whether the connection between the Cisco ONS 15540 and the client equipment is up. See the "Troubleshooting Client Side Transparent Interfaces" section on page 3-1 for information about the fields in this display.

Step 2 From node 1, use the **show interfaces wave** command to display the status of the trunk side laser on the transponder.

The **show interfaces wave** command indicates whether the connection between the Cisco ONS 15540 and the next optical fiber node is up. See the Chapter 4, "Troubleshooting Trunk Side Interfaces," for information about the fields in this display.

Step 3 From node 1, use the **ping** command and the IP address of the node 2 wave 0 OSC interface. The following **ping** command tests the connection between the processor on node 1, through the OSC wave 0 interface (west), to the processor on node 2.

If the connection fails, it could indicate a fiber failure in the west direction from node 1.

Step 4 From node 1, use the **ping** command and the IP address of the node 2, wave 1 OSC interface. The following **ping** command tests the connection between the processor on node 1, through the OSC wave 1 interface (east), to the processor on node 2.

The **ping** commands between the nodes proves the optical fiber connection between node 1 and node 2 in the west direction has failed and the standby connection in the east direction is working. It does not indicate if the individual channel connections have been misconfigured or one of the patch connections or components has failed.

For IP address configuration instructions for the OSC channel interface, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

If these four steps have not found the failed connection between nodes, continue with the following more disruptive connection loopback troubleshooting steps.

Caution The following troubleshooting steps for the individual channels and components of the Cisco ONS 15540 are disruptive to the client connections and can only be completed with login access to the client end-station equipment connected to the Cisco ONS 15540.

Step 5 From node 1, configure the transparent interface between the Cisco ONS 15540 and the client as a loopback connection using the instructions in the "Checking Connectivity" section on page 5-1.

Confirm the loopback configuration using the **show interfaces transparent** command. The field Loopback set should appear in the **show interfaces transparent** display.

From the client equipment connected to node 1, confirm the connection to the client appears as looped back. This proves the connection from the client to the transparent interface on node 1 is working.

Note Before continuing with the next loopback test, disable loopback on the transparent interface connected to the near end client.

Step 6 From node 2, configure the wave interface between the Cisco ONS 15540 and the far-end client loopback connection using the instructions in the "Checking Connectivity" section on page 5-1.

Confirm the loopback configuration using the **show interfaces wave** command.

The field Loopback set should appear in the **show interfaces wave** display.

From the client connection through node 1 to node 2, confirm the connection to the client is looped back. This proves the connection from the client to the wave interface on node 2 is working.

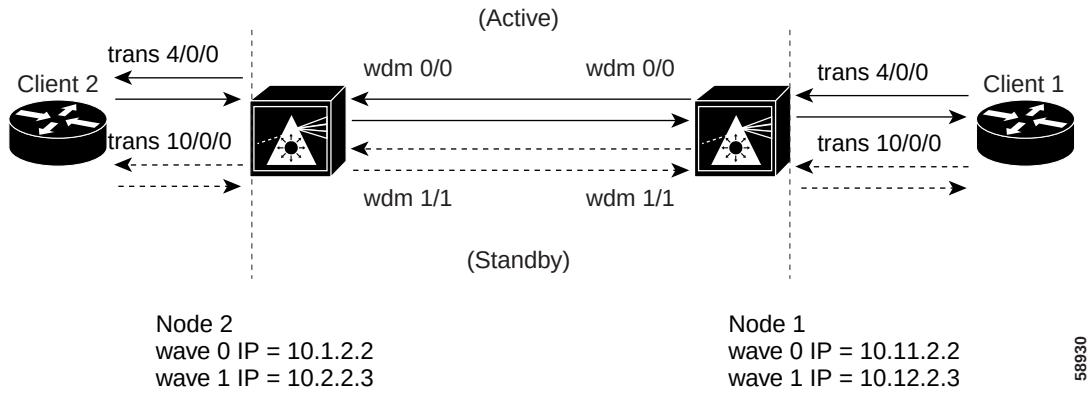
Step 7 From the client equipment connected to node 1, configure a loopback connection through the entire network end-to-end. This confirms the connection between the clients connected to node 1 and node 2 at both ends.

Troubleshooting Point-to-Point Topology with Line Card Protection

Figure 5-4 shows a line card protected topology with two nodes. Both nodes use channels 1-16 and use the following:

- Transparent interfaces 2/0/0 through 5/3/0 (active) on a west line card motherboard
- Transparent interfaces 8/0/0 through 11/3/0 (standby) on an east line card motherboard
- Mux/demux module wdm 0/0 out to the west
- Mux/demux module wdm 1/2 out to the east

Figure 5-4 Point-to-Point Network with Line Card Protection



For an example configuration of a line card protected point-to-point topology, refer to the *Cisco ONS 15540 ESP Planning Guide.*

To troubleshoot the configuration and status of the point-to-point connection with line card protection, use the following EXEC commands:

Command	Purpose
show interfaces transparent *slot/subcard/0*	Shows the status of the physical interfaces between the Cisco ONS 15540 and the clients.
show interfaces wave *slot/subcard*	Displays the status and configuration of the wave interface between Cisco ONS 15540 systems.
ping {*ip-address* | *hostname*}	Confirms the connection between OSC Wave interfaces and the system fiber connections.
[**no**] **loopback**	Enables and disables loopback on the interface.

Follow these general steps to troubleshoot point-to-point connections with line card protection between two end user clients:

Step 1 From node 1, use the **show interfaces transparent** command to display the connection between the transparent interface on the Cisco ONS 15540 and the client equipment.

The **show interfaces transparent** command indicates whether the connection between the Cisco ONS 15540 and the client equipment is up. See the "Troubleshooting Client Side Transparent Interfaces" section on page 3-1 for information about the fields in this display.

Step 2 From node 1, use the **show interfaces wave** command to display the connection status between the laser on the transponder all the way to the next Cisco ONS 15540 node.

The **show interfaces wave** command indicates whether the connection between the Cisco ONS 15540 and the neighboring node is up. See the Chapter 4, "Troubleshooting Trunk Side Interfaces," for information about the fields in this display.

Step 3 From node 1, use the **ping** command and the IP address of the node 2 wave 0 OSC channel interface. If the connection fails, as in the previous example, this could indicate a fiber failure in the west direction from node 1.

Step 4 From node 1, use the **ping** command and the IP address of the node 2, wave 1 OSC channel interface. The **ping** commands between the nodes proves the optical fiber connection between node 1 and node 2 in the west direction has failed and the standby connection in the east direction is working. It does not indicate if the individual channel connections have been misconfigured or one of the patch connections or components has failed.

For IP address configuration instructions for the OSC channel interface, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

If these four steps have not found the failed connection between the nodes, continue with the following more disruptive connection loopback troubleshooting steps.

Caution The following troubleshooting steps for the individual channels and components of the Cisco ONS 15540 are disruptive to the client connections and can only be completed with login access to the client end-station equipment connected to the Cisco ONS 15540.

Step 5 From node 1, configure the transparent interface between the Cisco ONS 15540 and the client as a loopback connection using the instructions in the "Checking Connectivity" section on page 5-1.

Confirm the loopback configuration using the **show interfaces transparent** command.

The field Loopback set should appear in the **show interfaces transparent** display.

From the client equipment connected to node 1, confirm the connection to the client appears as looped back. This proves the connection from the client to the transparent interface on node 1 is working.

Note Before continuing with the next loopback test, disable loopback on the transparent interface connected to the near end client.

Step 6 From node 2, configure the wave interface between the Cisco ONS 15540 and the far-end client loopback connection using the instructions in the "Checking Connectivity" section on page 5-1.

Confirm the loopback configuration using the **show interfaces wave** command. The field Loopback set should appear in the **show interfaces wave** display.

From the client connection through node 1 to node 2, confirm the connection to the client is looped back. This proves the connection from the client to the wave interface on node 2 is working.

Step 7 From the client equipment connected to node 1, configure a loopback connection through the entire network end-to-end. This confirms the connection between the clients connected to node 1 and node 2 at both ends.

Troubleshooting Hubbed Ring Topology with Splitter Protection

Figure 5-5 shows a network configured as a hubbed ring with splitter protection.

When a failure occurs between two nodes in a ring network, for example the failure between nodes 4 and 5 shown in Figure 5-5, alarms may appear on connections all around the network. For example, a "loss of signal" alarm may appear on the functioning connection between nodes 1 and 5 and a "loss of light" alarm may appear on the failed connection between nodes 4 and 5.

Note For splitter protected connections, alarms are only generated for the active side of the connection. Failures on the standby connection do not generate alarms.

For an example configuration of a splitter protected hubbed ring topology, refer to the *Cisco ONS 15540 ESP Planning Guide.*

Figure 5-5 Hubbed Ring Network with Splitter Protection

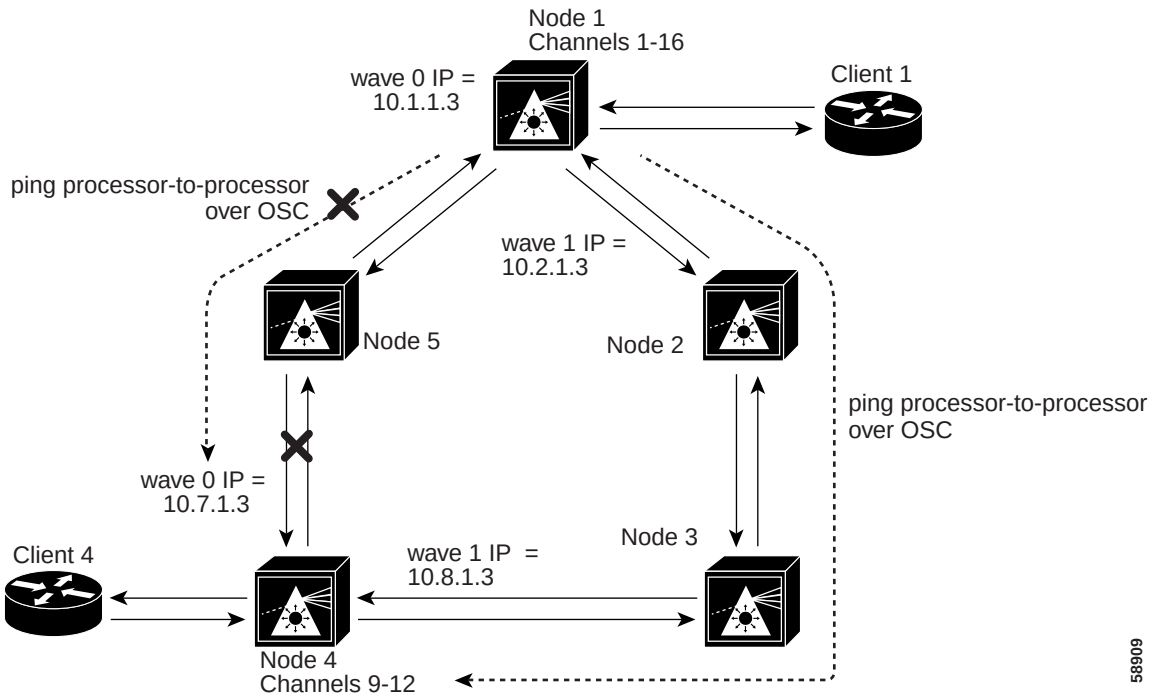


Figure 5-5 shows a splitter protected hubbed ring topology with five nodes. Node 1 and node 4 are configured as follows:

- Node 1—Channels 9-12 use the following:
  - Transparent interfaces 8/0/0 through 8/3/0 on a splitter protected line card motherboard
  - Mux/demux module wdm 0/0 out to the west
  - Mux/demux module wdm 1/0 out to the east
- Node 4—Channels 9-12 use the following:
  - Transparent interfaces 8/0/0 through 8/3/0 on a splitter protected line card motherboard
  - Mux/demux module wdm 0/2 out to the west
  - Mux/demux module wdm 1/2 out to the east

To troubleshoot the configuration and status of the optical connections in the hubbed ring with splitter protection, use the following EXEC commands:

Command	Purpose
show interfaces transparent *slot/subcard/0*	Shows the status of the physical interfaces between the Cisco ONS 15540 and the clients.
show interfaces wave *slot/subcard*	Displays the status and configuration of the wave interface between Cisco ONS 15540 systems.
ping {*ip-address* | *hostname*}	Confirms the connection between OSC wave interfaces and the system fiber connections.
[**no**] **loopback**	Enables and disables loopback on the interface.

Follow these steps to troubleshoot a splitter protected hubbed ring connection between two end user clients, shown in Figure 5-8:

Step 1 From node 1, use the **show interfaces transparent** command to display the connection between the transparent interface on the Cisco ONS 15540 and the client equipment connection.

The **show interfaces transparent** command indicates whether the connection between the Cisco ONS 15540 and the client equipment is up. See the "Troubleshooting Client Side Transparent Interfaces" section on page 3-1 for information about the fields in this display.

Step 2 From node 1, use the **show interfaces wave** command to display the status of the trunk side laser on the transponder.

The **show interfaces wave** command indicates whether the connection between the Cisco ONS 15540 and the next optical fiber node is up. See the Chapter 4, "Troubleshooting Trunk Side Interfaces," for information about the fields in this display.

Step 3 From node 1, use the **ping** command and the IP address of the node 4 wave 0 OSC interface (west).

If the connection fails, as in the previous example, this could indicate a fiber failure in the west direction from node 1.

Step 4 From node 1, use the **ping** command and the IP address of the node 4, wave 1 OSC interface (east). The **ping** commands between the nodes proves the optical fiber connection between node 1 and node 4 in the west direction has failed and the standby connection in the east direction is working. It does not indicate if the individual channel connections have been misconfigured or one of the patch connections or components has failed.

To determine which connections has failed, the connection between node 1 and node 5 or the connection between node 5 and node 4, use the same process to ping the processors over the OSC interface. This confirms the failure is a component of those two nodes or a cable in between node 5 and node 4.

For IP address configuration instructions for the OSC channel interface, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

If these four steps have not found the failed connection between nodes continue with the following more disruptive connection loopback troubleshooting steps.

Caution The following troubleshooting steps for the individual channels and components of the Cisco ONS 15540 are disruptive to the client connections and can only be completed with login access to the client end-station equipment connected to the Cisco ONS 15540.

Step 5 From node 1, configure the transparent interface between the Cisco ONS 15540 and the client as a loopback connection using the instructions in the "Checking Connectivity" section on page 5-1.

Confirm the loopback configuration using the **show interfaces transparent** command.

The field Loopback set should appear in the **show interfaces transparent** display.

From the client equipment connected to node 1, confirm the connection to the client appears as looped back. This proves the connection from the client to the transparent interface on node 1 is working.

Note Before continuing with the next loopback test, disable loopback on the transparent interface connected to the near end client.

Step 6 From node 4, configure the wave interface between the Cisco ONS 15540 and the far-end client loopback connection using the instructions in the "Checking Connectivity" section on page 5-1.

Confirm the loopback configuration using the **show interfaces wave** command. The field Loopback set should appear in the **show interfaces wave** display.

From the client connection through node 1 to node 4, confirm the connection to the client is looped back. This proves the connection from the client to the wave interface on node 4 is working.

Step 7 From the client equipment connected to node 4, configure a loopback connection through the entire network end-to-end. This confirms the connection between the clients connected to node 1 and node 2 at both ends.

Troubleshooting Hubbed Ring Topology with Line Card Protection

Figure 5-6 shows a network configured as a hubbed ring with line card protection.

When a failure occurs between two nodes in a ring network, for example the failure between nodes 4 and 5 shown in Figure 5-6, alarms may appear on connections all around the network. For example, a "loss of signal" alarm may appear on the functioning connection between nodes 1 and 5 and a "loss of light" alarm may appear on the failed connection between nodes 4 and 5.

For an example configuration of a line card protected hubbed ring topology, refer to the *Cisco ONS 15540 ESP Planning Guide.*

Figure 5-6 Hubbed Ring Network with Line Card Protection

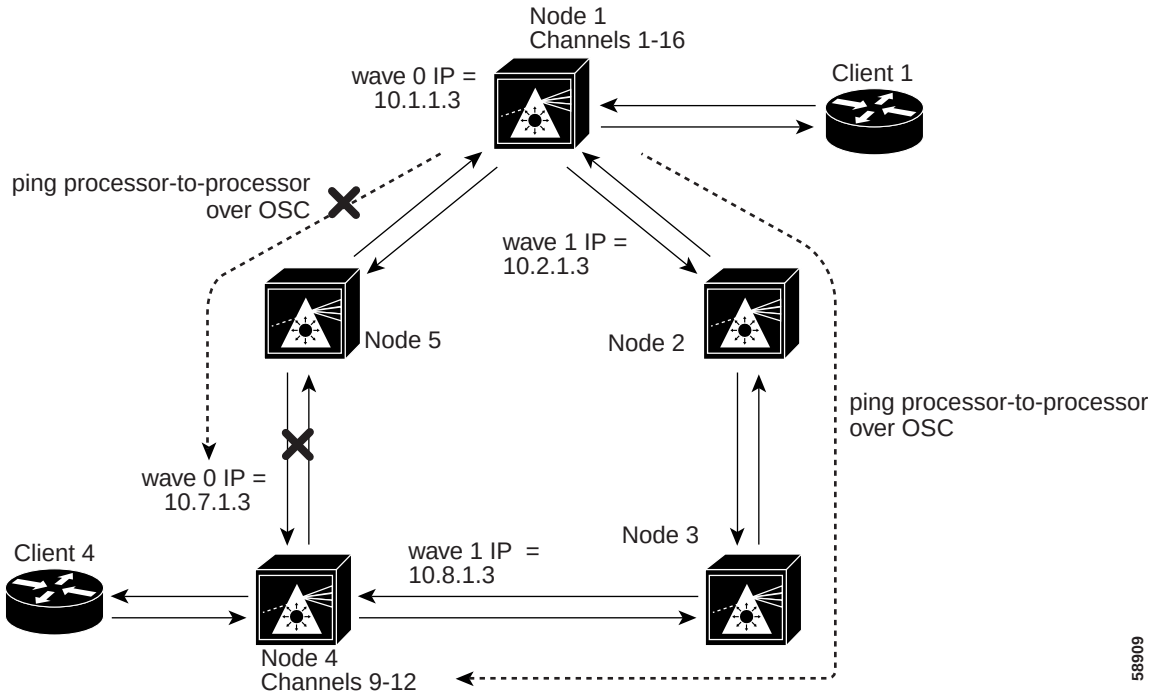


Figure 5-6 shows a line card protected hubbed ring topology with five nodes. Node 1 and node 4 are configured as follows:

- Node 1—Channels 9-12 use the following:
  - Transparent interfaces 4/0/0 through 4/3/0 (active) on a west line card motherboard
  - Transparent interfaces 10/0/0 through 10/3/0 (standby) on an east line card motherboard
  - Mux/demux module wdm 0/0 out to the west
  - Mux/demux module wdm 1/1 out to the east
- Node 4—Channels 9-12 use the following:
  - Transparent interfaces 8/0/0 through 8/3/0 (active) on a west line card motherboard
  - Transparent interfaces 10/0/0 through 10/3/0 (standby) on an east line card motherboard
  - Mux/demux module wdm 0/2 out to the west
  - mux/demux module wdm 1/3 out to the east

For a detailed description of this configuration, refer to the *Cisco ONS 15540 ESP Planning Guide*.

The following steps describe the troubleshooting process needed to find the failed connection between node 4 and node 5 in Figure 5-6. This failure causes the active connection between nodes 1 and 4, through node 5, to automatically switch to the standby connection through nodes 2 and 3.

To troubleshoot the configuration and status of the optical connections in the hubbed ring with line card protection, use the following EXEC commands:

Command	Purpose
show interfaces transparent *slot/subcard/0*	Shows the status of the physical interfaces between the Cisco ONS 15540 and the clients.
show interfaces wave *slot/subcard*	Displays the status and configuration of the wave interface between Cisco ONS 15540 systems.
ping {*ip-address* | *hostname*}	Confirms the connection between OSC wave interfaces and the system fiber connections.
[**no**] **loopback**	Enables and disables loopback on the interface.

Follow these general steps to troubleshoot an optical fiber network connection between two end user clients in a hubbed ring network with line card protection.

Step 1 From node 1, use the **show interfaces transparent** command to display the connection between the transparent interfaces on the Cisco ONS 15540 and the client equipment connection.

The **show interfaces transparent** command confirms whether the connection between the Cisco ONS 15540 and the client equipment is up. See the "Troubleshooting Client Side Transparent Interfaces" section on page 3-1 for information about the fields in this display.

Step 2 From node 1, use the **show interfaces wave** command to display the status of the trunk side laser on the transponder.

The **show interfaces wave** command indicates whether the connection between the Cisco ONS 15540 and the next optical fiber node is up.

Step 3 From node 1, use the **ping** command and the IP address of the node 4 wave 0 OSC interface. This tests the connection between the processor on node 1, through the OSC wave 0 interface (west), to the processor on node 4.

If the connection fails, this indicates a fiber failure in the west direction from node 1.

Step 4 From node 1, use the **ping** command and the IP address of the node 4, wave 1 OSC interface. This tests the connection between the processor on node 1, through the OSC wave 1 interface (east), to the processor on node 4.

The **ping** commands between the nodes proves the optical fiber connection between node 1 and node 4 in the west direction has failed and the standby connection in the east direction is working. It does not indicate if the individual channel connections have been misconfigured or one of the patch connections or components has failed.

To determine which connections have failed, the connection between node 1 and node 5 or the connection between node 5 and node 4, use the same process to ping the processors over the OSC interface. In this example, using the **ping** command to test the connection between node 1 and node 5 will work but the test from node 5 to node 4 will fail. This confirms the failure is a component of those two nodes or a cable in between node 5 and node 4.

If these four steps have not found the failed connection between nodes, continue with the following more disruptive connection loopback troubleshooting steps.

Caution The following troubleshooting steps for the individual channels and components of the Cisco ONS 15540 are disruptive to the client connections and can only be completed with login access to the client end-station equipment connected to the Cisco ONS 15540.

Step 5 From node 1, configure the transparent interface between the Cisco ONS 15540 and the client as a loopback connection using the instructions in the "Checking Connectivity" section on page 5-1.

Confirm the loopback configuration using the **show interfaces transparent** command.

The field Loopback set should appear in the **show interfaces transparent** display.

From the client connected to node 1, confirm the connection to the client is looped back. This proves the connection from the client to the transparent interface on node 1 is working.

Note Before continuing with the next loopback test, disable loopback on the transparent interface connected to the near end client.

Step 6 From node 4, configure the wave interface between the Cisco ONS 15540 and the far-end client as a loopback connection using the instructions in the "Checking Connectivity" section on page 5-1.

Confirm the loopback configuration using the **show interfaces wave** command.

The field Loopback set should appear in the **show interfaces wave** display.

From the client connection through node 1 to node 4, confirm the connection to the client is looped back. This proves the connection from the client to the wave interface on node 4 is working.

If the wave loopback test of node 4 fails on *all* channels 9-12 that could indicate one of the following failures:

- The DWDM mux/demux installed in node 4, slot 0/2, failed.
- The fiber optic connection to the west between nodes 4 and 5 failed.
- The line card motherboard failed.

If the wave loopback test of node 4 fails on only *one* channel, for example channel 12, that could indicate the client connection to the transponder module for channel 12 has failed or the transponder has failed.

Note Failure of the transponder module should have been found using the **show transparent** interface command.

From the client equipment connected to node 4, configure a loopback connection through the entire network end-to-end. This confirms the connection between the clients connected to node 1 and node 4 at both ends.

Troubleshooting Meshed Ring Topology with Splitter Protection

This section describes troubleshooting meshed ring network with splitter protection. A meshed ring is a physical ring that has the logical characteristics of a mesh. While traffic travels on a physical ring, the logical connections between individual nodes are meshed.

Figure 5-7 shows a network configured as a meshed ring with splitter protection.

When a failure occurs between two nodes in a ring network, for example the failure between nodes 3 and 4 shown in Figure 5-7, alarms may appear on connections all around the network. For example, a "loss of signal" alarm may appear on the functioning connection between nodes 1 and 4 and a "loss of light" alarm may appear on the failed connection between nodes 3 and 4.

Note For splitter protected connections, alarms are only generated for the active side of the connection. Failures on the standby connection do not generate alarms.

For an example configuration of a splitter protected meshed ring topology, refer to the *Cisco ONS 15540 ESP Planning Guide.*

Figure 5-7 Meshed Ring Network with Splitter Protection

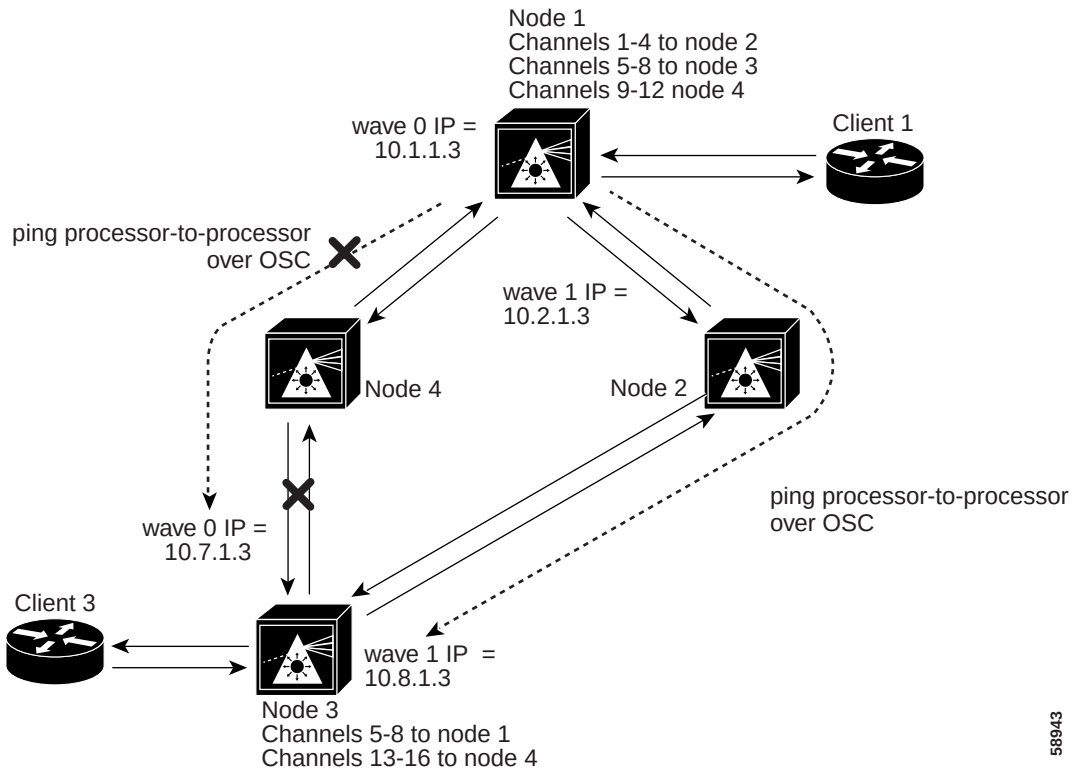


Figure 5-7 shows a splitter protected meshed ring topology with four nodes. Node 1 and node 3 are configured as follows:

- Node 1—Channels 5-8 use the following:
  - Transparent interfaces 5/0/0 through 5/3/0 on a splitter protected line card motherboard
  - Mux/demux module wdm 0/1 patched to wdm 0/0 out to the west
  - Mux/demux module wdm 1/1 patched to wdm 1/2 out to the east
- Node 3—Channels 5-8 use the following:
  - Transparent interfaces 5/0/0 through 5/3/0 on a splitter line card motherboard
  - Mux/demux module wdm 0/1 out to the west
  - mux/demux module wdm 1/1 out to the east

For an example of configuring a splitter protected meshed ring topology, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

To troubleshoot the configuration and status of the optical connections in the meshed ring with splitter protection, use the following EXEC commands:

Command	Purpose
show interfaces transparent *slot/subcard/0*	Shows the status of the physical interfaces between the Cisco ONS 15540 and the clients.
show interfaces wave *slot/subcard*	Displays the status and configuration of the wave interface between Cisco ONS 15540 systems.
ping {*ip-address* | *hostname*}	Confirms the connection between OSC wave interfaces and the system fiber connections.
[**no**] **loopback**	Enables and disables loopback on the interface.

Follow these steps to troubleshoot a meshed ring topology with splitter protection between two end user clients:

Step 1 From node 1, use the **show interfaces transparent** command to display the connection between the transparent interface on the Cisco ONS 15540 and the client equipment connection.

The **show interfaces transparent** command indicates whether the connection between the Cisco ONS 15540 and the client equipment is up. See the "Troubleshooting Client Side Transparent Interfaces" section on page 3-1 for information about the fields in this display.

Step 2 From node 1, use the **show interfaces wave** command to display the connection status between the laser on the transponder all the way to the next Cisco ONS 15540 node.

The **show interfaces wave** command indicates whether the connection between the Cisco ONS 15540 and the next optical fiber node is up. See the Chapter 4, "Troubleshooting Trunk Side Interfaces," for information about the fields in this display.

Step 3 From node 1, use the **ping** command and the IP address of the node 3 wave 0 OSC interface. This tests the connection between the processor on node 1, through the OSC wave 0 interface (west), to the processor on node 3.

If the connection fails, as in the previous example, this could indicate a fiber failure in the west direction from node 1.

Step 4 From node 1, use the **ping** command and the IP address of the node 3, wave 1 OSC interface. This tests the connection between the processor on node 1, through the OSC wave 1 interface (east), to the processor on node 3.

The **ping** commands between the nodes proves the optical fiber connection between node 1 and node 3 in the west direction has failed and the standby connection in the east direction is working. It does not indicate if the individual channel connections have been misconfigured or one of the patch connections or components has failed.

To determine which connection has failed, the connection between node 1 and node 4 or the connection between node 4 and node 3, use the same process to ping the processors over the OSC interface. In this example, using the **ping** command to test the connection between node 1 and node 4 will work but the test from node 4 to node 3 will fail. This confirms the failure is a component of those two nodes or a cable in between node 4 and node 3.

For IP address configuration instructions for the OSC channel interface, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

If these four steps have not found the failed connection between nodes, continue with the following more disruptive connection loopback troubleshooting steps.

Caution The following troubleshooting steps for the individual channels and components of the Cisco ONS 15540 are disruptive to the client connections and can only be completed with login access to the client end-station equipment connected to the Cisco ONS 15540.

Step 5 From node 1, configure the transparent interface between the Cisco ONS 15540 and the client as a loopback connection using the instructions in the"Checking Connectivity" section on page 5-1.

Confirm the loopback configuration using the **show interfaces transparent** command. The field Loopback set should appear in the **show interfaces transparent** display.

From the client equipment connected to node 1, confirm the connection to the client appears as looped back. This proves the connection from the client to the transparent interface on node 1 is working.

Note Before continuing with the next loopback test, disable loopback on the transparent interface connected to the near end client.

Step 6 From node 3, configure the wave interface between the Cisco ONS 15540 and the far-end client loopback connection using the instructions in the "Checking Connectivity" section on page 5-1.

Confirm the loopback configuration using the **show interfaces wave** command.

The field Loopback set should appear in the **show interfaces wave** display.

From the client connection through node 1 to node 3, confirm the connection to the client is looped back. This proves the connection from the client to the wave interface on node 3 is working.

Step 7 From the client equipment connected to node 3, configure a loopback connection through the entire network end-to-end. This confirms the connection between the clients connected to node 1 and node 3 at both ends.

Troubleshooting Meshed Ring Topology with Line Card Protection

This section describes troubleshooting a connection over a meshed ring network with line card protection.

Figure 5-8 shows a network configured as a meshed ring with line card protection.

When a failure occurs between two nodes in a ring network, for example the failure between nodes 3 and 4 shown in Figure 5-8, alarms may appear on connections all around the network. For example, a "loss of signal" alarm may appear on the functioning connection between nodes 1 and 4 and a "loss of light" alarm may appear on the failed connection between nodes 3 and 4.

For an example configuration of a line card protected meshed ring topology, refer to the *Cisco ONS 15540 ESP Planning Guide.*

Figure 5-8 Meshed Ring Network with Line Card Protection

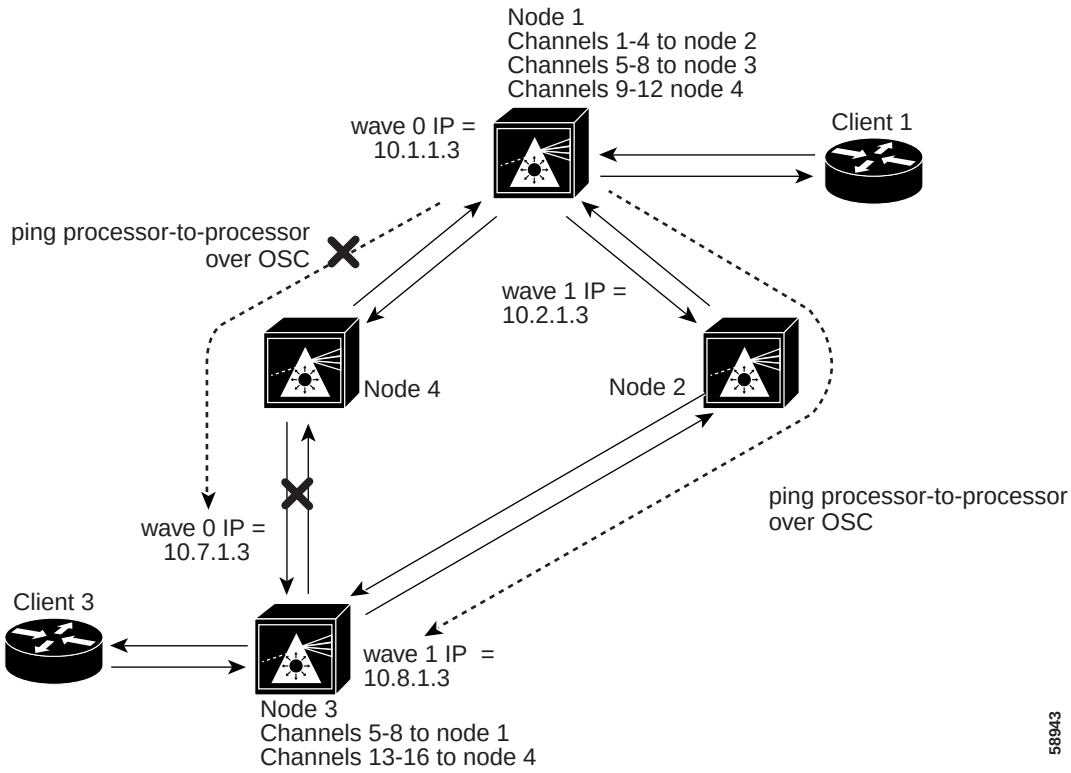


Figure 5-8 shows a line card protected meshed ring topology with four nodes. Node 1 and node 3 are configured as follows:

- Node 1—Channels 5-8 use the following:
  - Transparent interfaces 3/0/0 through 3/3/0 (active) on a west line card motherboard
  - Transparent interfaces 5/0/0 through 5/3/0 (standby) on an east line card motherboard
  - Mux/demux module wdm 0/1 patched to wdm 0/0 out to the west
  - Mux/demux module wdm 1/0patched to wdm 1/3 out to the east
- Node 3—Channels 5-8 use the following:
  - Transparent interfaces 3/0/0 through 3/3/0 (active) on a west line card motherboard
  - Transparent interfaces 5/0/0 through 5/3/0 (standby) on an east line card motherboard
  - Mux/demux module wdm 0/1 patched to wdm 0/3 out to the west
  - Mux/demux module wdm 1/0 patched to wdm 1/2 out to the east

For a detailed description of this configuration, refer to the *Cisco ONS 15540 ESP Planning Guide*.

To troubleshoot the configuration and status of the optical connections in the meshed ring with line card protection, use the following EXEC commands:

Command	Purpose
show interfaces transparent *slot/subcard/0*	Shows the status of the physical interfaces between the Cisco ONS 15540 and the clients.
show interfaces wave *slot/subcard*	Displays the status and configuration of the wave interface between Cisco ONS 15540 systems.
ping {*ip-address* | *hostname*}	Confirms the connection between OSC wave interfaces and the system fiber connections.
[**no**] **loopback**	Enables and disables loopback on the interface.

Follow these steps to troubleshoot a line card protected meshed ring optical fiber network connection between two end user clients:

Step 1 From node 1, use the **show interfaces transparent** command to display the connection between the transparent interface on the Cisco ONS 15540 and the client equipment connection.

The **show interfaces transparent** command indicates whether the connection between the Cisco ONS 15540 and the client equipment is up. See the "Troubleshooting Client Side Transparent Interfaces" section on page 3-1 for information about the fields in this display.

Step 2 From node 1, use the **show interfaces wave** command to display the connection status between the laser on the transponder all the way to the next Cisco ONS 15540 node.

The **show interfaces wave** command indicates whether the connection between the Cisco ONS 15540 and the next optical fiber node is up. See the Chapter 4, "Troubleshooting Trunk Side Interfaces," for information about the fields in this display.

Step 3 From node 1, use the **ping** command and the IP address of the node 3 wave 0 OSC interface. This tests the connection between the processor on node 1, through the OSC wave 0 interface (west), to the processor on node 3.

If the connection fails, as in the previous example, this could indicate a fiber failure in the west direction from node 1.

Step 4 From node 1, use the **ping** command and the IP address of the node 3, wave 1 OSC interface. This tests the connection between the processor on node 1, through the OSC wave 1 interface (east), to the processor on node 3.

The **ping** commands between the nodes proves the optical fiber connection between node 1 and node 4 in the west direction has failed and the standby connection in the east direction is working. It does not indicate if the individual channel connections have been misconfigured or one of the patch connections or components has failed.

To determine which connection has failed, the connection between node 1 and node 4 or the connection between node 4 and node 3, use the same process to ping the processors over the OSC interface. In this example, using the **ping** command to test the connection between node 1 and node 4 will work but the test from node 4 to node 3 will fail. This confirms the failure is a component of those two nodes or a cable between node 4 and node 3.

For IP address configuration instructions for the OSC channel interface, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

If these four steps have not found the failed connection between nodes, continue with the following more disruptive connection loopback troubleshooting steps.

Caution The following troubleshooting steps for the individual channels and components of the Cisco ONS 15540 are disruptive to the client connections and can only be completed with login access to the client end-station equipment connected to the Cisco ONS 15540.

Step 5 From node 1, configure the transparent interface between the Cisco ONS 15540 and the client as a loopback connection using the instructions in the "Checking Connectivity" section on page 5-1.

The field Loopback set should appear in the **show interfaces transparent** display.

From the client equipment connected to node 1, confirm the connection to the client appears as looped back. This proves the connection from the client to the transparent interface on node 1 is working.

Note Before continuing with the next loopback test, disable loopback on the transparent interface connected to the near end client.

Step 6 From node 3, configure the wave interface between the Cisco ONS 15540 and the far-end client loopback connection using the instructions in the "Checking Connectivity" section on page 5-1.

Confirm the loopback configuration using the **show interfaces wave** command.

The field Loopback set should appear in the **show interfaces wave** display.

From the client connection through node 1 to node 3, confirm the connection to the client is looped back. This proves the connection from the client to the wave interface on node 3 is working.

Step 7 From the client equipment connected to node 3, configure a loopback connection through the entire network end-to-end. This confirms the connection between the clients connected to node 1 and node 3 at both ends.

CHAPTER 6

Troubleshooting the Cisco ONS 15540 Processor Card

This chapter provides troubleshooting information about the Cisco ONS 15540 processors.

The Cisco ONS 15540 uses a fixed optical backplane between the client side transponder modules and the trunk side mux/demux modules. This minimizes the required functionality of the processor card. The processor card is used primarily to boot the system, provide Cisco IOS software version and download control, and provide APS redundancy and environmental monitoring mechanisms. In a redundant system, the processor cards monitor each other using the backplane Ethernet signals.

Note There is no switch fabric on the Cisco ONS 15540 processors.

The chapter includes the following sections:

- Verifying Processor Card Configuration, page 6-1
- Recovering a Lost Password, page 6-4
- Verifying NME Interface Configurations, page 6-5
- Troubleshooting Processor Card Memory, page 6-7
- Verifying Hardware and Software Versions, page 6-8
- Verifying Hardware and Software Compatibility, page 6-10
- Troubleshooting Redundant Processor Cards, page 6-13
- Checking the DDTs Database and Release Notes for Workarounds, page 6-17

Note For information on slot assignments, processor card LEDs, alarm condition clear and reset button, interrupt clear and reset button, NME LEDs, and cabling, refer to the *Cisco ONS 15540 ESP Hardware Installation Guide*. For default configuration of the various modules, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference.*

Verifying Processor Card Configuration

To display the processor configuration and status, use the **show running-config** command.

Command	Purpose
show running-config	Shows all components of the processor running a configuration.

The following example shows the **show running-config** command, which displays all the components of the processor configuration. For a detailed description of this command, refer to the *Cisco IOS Configuration Fundamentals Command Reference*.

```
Switch# show running-config
Building configuration...

Current configuration : 2773 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
boot bootldr bootflash:ons15540-i-mz.Apr18
no logging console
enable password lab
!
filter 1/0 1 8
ip subnet-zero
ip host-routing
no ip finger
no ip domain-lookup
!
oscp timer hello-interval  300
oscp timer inactivity-factor 25
oscp timer hello-holddown 50
patch Thru1/0 Wdm1/1
patch Thru1/1 Wdm1/2
!
!
interface Transparent3/0/0
 mtu 1514
 no ip address
 shutdown
 monitor enable
 encap sonet rate oc3
!

[Information deleted]

!
interface Wave3/0
 mtu 1514
 no ip address
 shutdown
!

[Information deleted]

!
```

```
interface Wdm1/0
 mtu 1514
 no ip address

[Information deleted]

!
interface Wavepatch3/0/0
 mtu 1514
 no ip address
 shutdown

[Information deleted]

!
interface Filter1/0/0
 mtu 1514
 no ip address

[Information deleted]

!
interface Thru1/0
 mtu 1514
 no ip address

[Information deleted]

!
interface FastEthernet0
 ip address 172.20.42.225 255.255.255.0
 duplex auto
 speed auto
!
ip default-gateway 172.20.42.206
ip classless
no ip http server
!
cdp timer 200
cdp holdtime 120
snmp-server engineID local 80000009030000AB0000007C
snmp-server community public RW
snmp-server enable traps rf
!
line con 0
 transport input none
line aux 0 1
line vty 0 4
 exec-timeout 0 0
 password lab
 login
 length 0
!
end
```

Recovering a Lost Password

This section describes the procedure to recover a lost login or to enable a password. The procedure differs depending on the platform and the software used, but in all cases, password recovery requires that the system be taken out of operation and powered down.

If you need to perform the following procedure, make certain that there are secondary systems that can temporarily serve the functions of the system undergoing the procedure. If this is not possible, advise all potential users and, if possible, perform the procedure during low-use hours.

Note Make a note of your password, and store it in a secure place.

All of the procedures for recovering lost passwords depend on changing the configuration register of the system. This is done by reconfiguring the system software.

More recent Cisco platforms run from Flash memory or are netbooted from a network server and can ignore the contents of NVRAM (nonvolatile random-access memory) when booting. By ignoring the contents of NVRAM, you can bypass the configuration file (which contains the passwords) and gain complete access to the system. You can then recover the lost password or configure a new one.

Note If your password is encrypted, you cannot recover it. You must configure a new password.

Follow these steps to recover a password:

Step 1 Enter the **show version** command and the configuration register value in the privileged EXEC mode. The default value is 0x2102.

Step 2 Power up the Cisco ONS 15540.

Step 3 Press the **Break** key sequence or send a break signal, which is usually **^] w**ithin 60 seconds of turning the system on. If you do not see the `>` prompt with a system name, the terminal is not sending the correct break signal. In that case, check the terminal or terminal emulation setup.

Step 4 Enter the **confreg** command at the `>` prompt.

Step 5 Answer **yes** to the `Do you wish to change configuration [y/n]?` prompt.

Step 6 Answer **no** to all the questions that appear until you reach the `Ignore system config info [y/n]` prompt. Answer **yes**.

Step 7 Answer **no** to the remaining questions until you reach the `Change boot characteristics [y/n]?` prompt. Answer **yes**.

Step 8 Enter **2** at the `enter to boot:` prompt.

Step 9 Answer **no** to the `Do you wish to change configuration [y/n]?` prompt.

Step 10 Enter the **reset** command at the `rommon>` prompt.

Step 11 Enter the **enable** command at the `Switch>` prompt. You are in enable mode and see the `Switch#` prompt.

Step 12 Enter the **show startup-config** command to view your password.

Step 13 Proceed to Step 16 if your password is clear text. Or, continue with Step 14 if your password is encrypted.

Step 14 Enter the **configure memory** command to copy the NVRAM into memory if your password is encrypted.

Step 15 Enter the **copy running-config startup-config** command.

Step 16 Enter the **configure terminal** command.

Step 17 Enter the **enable secret** *password* command.

Step 18 Enter the **config-registe**r *value* command, where *value* is whatever value you entered in Step 1.

Step 19 Enter the **exit** command to exit configuration mode.

Step 20 Enter the **copy running-config startup-config** command.

Step 21 Enter the **reload** command at the prompt.

Verifying NME Interface Configurations

The administration interfaces provide simple command-line interfaces to all internal management and debugging facilities of the processor. To manage and debug the processor, you can use the NME (network management Ethernet) interface, the console port, and the auxiliary port.

For cable connection information for each of these interface ports, refer to the *Cisco ONS 15540 ESP Hardware Installation Guide*. For initial configuration information, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

The NME interface has a full duplex, auto sensing connection with troubleshooting LEDs on the processor faceplate.

You can configure and monitor the NME connection using the CLI. The NME connection appears in the configuration as FastEthernet 0 or FastEthernet 1 depending on the slot where the processor is installed.

To display the NME FastEthernet module configuration and status, use the following commands:

Command	Purpose
show interfaces FastEthernet 0	Displays the status of the physical interface.
show controllers	Displays the interface memory management and error counters on the FastEthernet interface.

Follow these steps to verify the NME interface:

Step 1 Use the **show interfaces FastEthernet 0** *slot/subcard/port* command to check the NME interface configuration.

```
Switch# show interfaces FastEthernet 0
FastEthernet0 is up, line protocol is up
  Hardware is AmdFE, address is 0000.ab00.0000 (bia 0000.ab00.0000)
  Internet address is 172.20.42.118/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 10Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
```

```
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   222 packets input, 15877 bytes
   Received 194 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored 0 abort
   0 watchdog
   0 input packets with dribble condition detected
   28 packets output, 3384 bytes, 0 underruns(0/0/0)
   2 output errors, 0 collisions, 1 interface resets
   0 babbles, 0 late collision, 0 deferred
   2 lost carrier, 0 no carrier
```

Step 2 Check the FastEthernet field to see whether the interface is up. If it is down, check for the following:

- Disconnected or faulty cabling. Check cables.
- Hardware failure. Swap hardware.

If administratively down, the interface has been administratively taken down. Use the **no shutdown** interface configuration command to reenable the interface.

Step 3 Check the line protocol field to see whether the status is up.

If the interface is down, the line protocol software processes might have determined that the line is unusable or the local or remote interface might be misconfigured. See if the interface can be brought up by following the recommendations in Step 2.

Step 4 Check the duplex mode field. It should match the speed of the interface and be configured as auto-negotiation.

Step 5 Check the last input and last output fields. They show the number of hours, minutes, and seconds since the last packet was successfully received or transmitted by the interface.

Step 6 Check the output hang field. It shows the number of hours, minutes, and seconds since the last reset caused by a lengthy transmission.

Step 7 Check the CRC field. The presence of many CRC errors, but not many collisions, indicates excessive noise. If the number of errors is too high, check the cables for damage. If you are using UTP cable, make sure you are using Category 5 cables and not another type, such as Category 3.

Note Errors and the input and output difference should not exceed 0.5 to 2.0 percent of traffic on the interface.

Step 8 Check the collisions fields. These numbers indicate packet collisions and these numbers should be very low. The total number of collisions, with respect to the total number of output packets, should be 0.1 percent or less.

Step 9 Check the late collisions fields. Late collisions should never occur in a properly designed Ethernet network. They usually occur when Ethernet cables are too long or when there are too many repeaters in the network.

Step 10 Check carrier fields. These numbers indicate a lost carrier detect signal and can be caused by a malfunctioning interface that is not supplying the transmit clock signal or by a cable problem. If the system notices that the carrier detect line of an interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.

Step 11 Check the buffer fields. These numbers indicate the number of received packets discarded because there was no buffer space. Broadcast storms on Ethernet networks, and bursts of noise on serial lines, are often responsible for no-input buffer events.

Step 12 Check the FastEthernet field to see whether the interface is up. If it is down, see if the interface can be brought up by following the recommendations in Step 2. If administratively down, the interface has been administratively taken down. Use the **no shutdown** interface configuration command to reenable the interface.

If you determine that the connection is configured incorrectly, refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference*.

In addition, you can use the **show controllers** command to troubleshoot the status of the NME interface configuration:

```
Switch# show controllers fastethernet 0
Interface FastEthernet0
Hardware is AMD Laguna
ADDR: 60B31408, FASTSEND: 0, MCI_INDEX: 0
DIST ROUTE ENABLED: 0
Route Cache Flag: 1
 LADRF=0x0000 0x0100 0x0000 0x0000
 CSR0  =0x00000072, CSR3  =0x00001044, CSR4  =0x0000491D, CSR15 =0x00000180
 CSR80 =0x00009900, CSR114=0x00000000, CRDA  =0x04D86460, CXDA  =0x04D866C0
 BCR9 =0x00000000 (half-duplex)
 CSR5  =0x00000001, CSR7  =0x000008A8, CSR100=0x0000F000, CSR125=0x00005C3C
 BCR2  =0x00000000, BCR9  =0x00000000, BCR18 =0x00001981, BCR22 =0x0000FF06
 BCR25 =0x00000017, BCR26 =0x0000000C, BCR27 =0x00000000, BCR32 =0x00004800
 HW filtering information:
  Promiscuous Mode Disabled, PHY Addr Enabled, Broadcast Addr Enabled
  PHY Addr=0000.AB00.0000, Multicast Filter=0x0000 0x0100 0x0000 0x0000
 amdp2_instance=0x60B32F98, registers=0x46000000, ib=0x4D86180
 rx ring entries=64, tx ring entries=128
 rxring=0x4D861E0, rxr shadow=0x60B331A4, rx_head=40, rx_tail=0
 txring=0x4D86620, txr shadow=0x60B332D0, tx_head=10, tx_tail=10, tx_count=0
 Software MAC address filter(hash:length/addr/mask/hits):
 spurious_idon=0, filtered_pak=0, throttled=0, enabled=0, disabled=0
 rx_framing_err=0, rx_overflow_err=0, rx_buffer_err=0, rx_bpe_err=0
 rx_soft_overflow_err=0, rx_no_enp=0, rx_discard=0, rx_miss_count=0
 tx_one_col_err=0, tx_more_col_err=0, tx_no_enp=0, tx_deferred_err=0
 tx_underrun_err=0, tx_late_collision_err=0, tx_loss_carrier_err=2
 tx_exc_collision_err=0, tx_buff_err=0, fatal_tx_err=0
 hsrp_conf=0, need_af_check=0
 tx_limited=0(128)
 PHY registers:
  Register 0x00:   1000  786D  0000  6B60  01E1  0021  0004  2001
  Register 0x08:   0000  0000  0000  0000  0000  0000  0000  0000
  Register 0x10:   0013  0004  186A  001E  0440        2004  0001  0200
  Register 0x18:   0008  0000  0000  0000
```

Troubleshooting Processor Card Memory

To troubleshoot the processor memory, use the following commands:

Command	Purpose
show flash	Displays the configuration register value.

Command	Purpose
show memory	Shows statistics about the Cisco ONS 15540 memory, including free pool statistics.
show buffers	Displays statistics for the buffer pools on the Cisco ONS 15540.

Troubleshooting Cisco ONS 15540 processor card memory is the same as troubleshooting any Cisco route processor. You can refer to the document *Troubleshooting Hardware and Booting Problems* at the following URL: http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1903.htm.

If the Cisco ONS 15540 fails, it is sometimes useful to get a full copy of the memory image, called a *core dump*, to identify the cause of the failure. Core dumps are generally only useful to your technical support representative. For troubleshooting information relating to system management and information about creating core dumps, refer to the *Cisco IOS Configuration Fundamentals Command Reference*.

Verifying Hardware and Software Versions

A common problem is an incompatibility between a hardware module and the Cisco IOS software version needed to perform a particular function. This section describes troubleshooting that problem.

Display the hardware and software versions to ensure that they are the most recent. Very old hardware and software versions (two or three versions back) can have caveats that have been fixed in more recent versions. Use the following EXEC commands to display version information:

Command	Purpose
show version	Displays the software version information.
show hardware [**detail**]	Displays detailed hardware information including revision level and version.

To verify hardware and software versions, use the following steps:

Step 1 Use the **show version** command to display the system software version on the active processor.

```
Switch# show version

  Cisco Internetwork Operating System Software
  IOS (tm) ONS-15540 Software (manopt-M0-M), 12.1(X:X)
  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(X:X)
  BOOTFLASH:ONS-15540 Software (manopt-M0-M), 12.1(X:X)

  Switch uptime is 30 minutes
  System returned to ROM by power-on
  System image file is "tftp://test/eng/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
```

Step 2 Verify the ROM field. It indicates the release of Cisco IOS software loaded and running on the active processor.

Step 3 Use the **show hardware** command to display the hardware revision levels for the processors.

```
Switch# show hardware
--------------------------------------------------------------------------------
 named Switch, Date: 04:36:18 UTC Fri Apr 20 2001
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
➔ Slot Controller Type    Part No.   Rev Serial No.  Mfg. Date  RMA No. H/W Ver.
---- ------------------ ---------- --- ------------ ---------- ------- ----------
1    Mx-DMx-Mthrbd                                  01/01/2000 0x00    0.0
3    XpndrMotherboard                               01/01/2000 0x00    0.0
6    Queens CPU         73-5621-02 03  CAB0505GZHD 02/16/2001 0x00    2.1
7    Queens CPU         73-5621-02 03  CAB0505GZHV 02/16/2001 0x00    2.1

--------------------------------------------------------------------------------
Back-Plane EEPROM
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Model     Ver Serial No. MAC-Address       MAC-Size RMA No. RMA Code MFG-Date
--------- --- ---------- ----------------- -------- ------- -------- -----------
          0.0            00-ab-00-00-00-   1        0x00    0x00     01/01/2000

--------------------------------------------------------------------------------
Power-Supply Module
--------------------------------------------------------------------------------
Primary Power-Supply is : Not working
Backup  Power-Supply is : Not working
```

Step 4 Verify that the hardware versions listed in the H/W Ver column for the processors in slots 6 and 7 are the same. If the hardware versions are not the same, continue with the "Verifying Hardware and Software Compatibility" section on page 6-10.

Step 5 Use the **show hardware detail** command to display detailed information about the processor hardware, including the functional image versions.

```
Switch# show hardware detail
--------------------------------------------------------------------------------
 named Switch, Date: 04:36:29 UTC Fri Apr 20 2001
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Slot Number             : 1
Controller Type         : Mx-DMx-Mthrbd
On-Board Description    :
Orderable Product Number:
Board Part Number       :
Board Revision          :
Serial Number           :
Manufacturing Date      : 01/01/2000
Hardware Version        : 0.0
RMA Number              : 0x00
RMA Failure Code        : 0x00
```

```
Functional Image Version: 2.18

--------------------------------------------------------------------------------

[Information Deleted]

--------------------------------------------------------------------------------
Slot Number             : 6
Controller Type         : Queens CPU
On-Board Description    : Queens_CPU_PHASE_0
Orderable Product Number: N/A
Board Part Number       : 73-5621-02
Board Revision          : 03
Serial Number           : CAB0505GZHD
Manufacturing Date      : 02/16/2001
➔ Hardware Version        : 2.1
RMA Number              : 0x00
RMA Failure Code        : 0x00
➔ Functional Image Version: 1.8

--------------------------------------------------------------------------------
Slot Number             : 7
Controller Type         : Queens CPU
On-Board Description    : Queens_CPU_PHASE_0
Orderable Product Number: N/A
Board Part Number       : 73-5621-02
Board Revision          : 03
Serial Number           : CAB0505GZHV
Manufacturing Date      : 02/16/2001
➔ Hardware Version        : 2.1
RMA Number              : 0x00
RMA Failure Code        : 0x00
➔ Functional Image Version: 1.11

--------------------------------------------------------------------------------

[Information Deleted]
```

Step 6 Verify that the Hardware Version and Functional Image Version fields for the processors in slots 6 and 7 are the same. If they are not the same, continue with the following process to confirm that they are compatible.

Verifying Hardware and Software Compatibility

You can verify your hardware and software version compatibility by using the following EXEC command to display processor compatibility information:

Command	Purpose
show redundancy capability	Displays the software version compatibility information.

To verify hardware and software compatibility of the processors and modules, use the following steps:

Step 1 Use the **show redundancy capability** command to display the system software version compatibility with the various modules installed.

```
Switch# show redundancy capability

CPU capability support

 Active CPU  Sby CPU    Sby Compat        CPU capability description
 ---------- ---------- ---------- ----------------------------------------
➔    96 MB      96 MB   OK         CPU DRAM size
➔    32 MB      32 MB   OK         CPU PMEM size
    512 KB     512 KB   OK         CPU NVRAM size
     16 MB      16 MB   OK         CPU Bootflash size
➔    2.1        2.1     OK         CPU hardware major.minor version
➔    1.129      1.129   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
 --More--         Active CPU  Sby CPU   Sby Compat  Drv ID     Driver description
 ---------- ---------- ---------- ------ ----------------------------------
    1.1        1.1     OK         0x1007 32-ch Mux/Demux
    1.1        1.1     OK         0x1008 Fixed 4-ch Mux/Demux, no OSC
    1.1        1.1     OK         0x1009 Fixed 8-ch Mux/Demux, no OSC
    1.1        1.1     OK         0x100A Modular 4-ch Mux/Demux, no OSC
    1.1        1.1     OK         0x100B Modular 8-ch Mux/Demux, no OSC
    1.1        1.1     OK         0x100C 32-ch Array Wave Guide
    1.1        1.1     OK         0x100D Mux/Demux Motherboard
    1.1        1.1     OK         0x100E Modular 4-ch Mux/Demux plus OSC
    1.1        1.1     OK         0x100F Modular 8-ch Mux/Demux plus OSC
    1.1        1.1     OK         0x1010 Mux-Demux Motherboard, no OSC
    1.1        1.1     OK         0x1011 Line Card Motherboard, no splitter

➔ Software sync client versions, listed as version range X-Y.
 X indicates the oldest peer version it can communicate with.
 Y indicates the current sync client version.
 Sync client counts:Active=2, Standby=2

 Active CPU  Sby CPU   Sby Compat  Cl ID  Redundancy Client description
 ---------- ---------- ---------- ----- ----------------------------------
➔ ver  1-1   ver  1-1   OK         17    CPU Redundancy
➔ ver  1-1   ver  1-1   OK         6     OIR Client

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
 serial_number_str          YES   XXXXXXXXX            XXXXXXXXX
```

```
 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             YES   0                    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    17248                42412
 user_track_string           YES   lab                  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   00016442e6aa         00016442e6aa
 cpu_number                  OK    0                    1
 optical_backplane_type      YES   255                  255
Switch#
```

Step 2 Check the CPU memory sizes and versions in the column, CPU capability description column. The numbers in the columns Active CPU and Sby CPU (Standby CPU) columns should match. If not, check the Sby Compat (Standby Compatibility) column. If this column indicates the values are OK, then these values will function as compatible redundant processors. If not, swap the processors with versions that are compatible.

Step 3 Check the CPU hardware major.minor versions and CPU functional major.minor versions in the column, CPU capability description column. The numbers in the Active CPU and Sby CPU (Standby CPU) columns should match. If not, check the Sby Compat (Standby Compatibility) columns. If this column indicates the values are OK, then these values will function as compatible redundant processors. If not, swap the processors with versions that are compatible.

Step 4 Check the information in the Linecard driver section of the display. This section shows the compatibility of the software versions installed on the active and standby processors with the various modules installed in the system.

Step 5 Check the Sby Compat (Standby Compatibility) and the Driver description columns. An OK in the Sby Compat column indicates the software version installed on the processors supports the drivers on the modules listed.

Step 6 Check the Software sync client version section of the display. The Active CPU, Sby CPU and Redundancy Client description columns indicate the software versions the two processors can use to synchronize their configurations. The version range in the display, shown as X-Y, indicates oldest-current peer client versions. For example, if the version lists 1-2, that indicates version 1 is the oldest version that the current version 2 could synchronize with its configuration.

Step 7 Check the Backplane IDPROM comparison section of the display. Check the Match column. This indicates which elements match, are acceptable, or fail. Some elements do not match but the range is acceptable. For example, the crc16 elements fields never match because the information in the IDPROMs of the two processors are different so the checksums never match. But they do appear as OK or compatible.

If any of the drivers are not supported or appear as OK, try updating the images installed on the processors. Use the information in the "Checking the DDTs Database and Release Notes for Workarounds" section on page 6-17 to upgrade to a more recent version. That should solve a processor image compatibility problem.

Troubleshooting Redundant Processor Cards

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

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

- If the running configurations on the active and standby processor cards match, the new active processor card uses the running configuration file.
- If the running configurations on the active and standby processors do not match, the new active processor card uses the last saved configuration file in its NVRAM (not the NVRAM of the former active processor card).

The former active processor card then becomes the standby processor.

Note If the standby processor card is unavailable, a major alarm is reported. Use the **show facility-alarm status** command to display the redundancy alarm status.

For redundant processor cards to function correctly, your Cisco ONS 15540 processor cards must meet the following requirements:

- Both processor cards must have compatible hardware configurations.
- Both processor cards must have compatible releases of Cisco IOS software.

A common error you may encounter is the incompatibility of hardware modules and the Cisco IOS software version needed to perform a particular function.

Verifying Hardware and Software Versions of Redundant Processor Cards

To troubleshoot the processor card hardware and software versions for redundancy, use the following commands:

Command	Purpose
show version	Displays the processor card software version information.
show redundancy	Displays the hardware and software configurations of the active and standby processor cards.

To troubleshoot the hardware and software versions on redundant processor cards, use the following steps:

Step 1 Use the **show version** command to display the system software version on the active processor card as described in the "Verifying Hardware and Software Versions" section on page 6-8.

Step 2 Use the **show redundancy** command to check the configuration and status of the active and standby processor card.

```
Switch# show redundancy

Redundant system information
-----------------------------
Available Uptime:             50 weeks, 5 days, 6 hours, 14 minutes
Time since last switchover:   30 weeks, 3 days, 2 hours, 20 minutes
Switchover Count:             2

Inter-CPU Communication State:UP

→ Last Running Config sync:     3 hours, 5 minutes
→ Running Config sync status:   In Sync
→ Last Startup Config sync:     1 week, 3 days, 4 hours, 19 minutes
  Startup Config sync status:   In Sync

  Last Restart Reason:          Normal boot

→ This CPU is the Active CPU.
  ------------------------------
  Slot:                         6
  Time since CPU Initialized:   35 weeks, 5 days, 1 hours, 42 minutes
  Image:                        Version 12.1(20010328:195418) 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:   7 hours, 14 minutes
  Image:                        Version 12.1(20010328:195418) ons15540-i-mz
→ Software Redundancy State:    STANDBY HOT
→ Hardware State:               STANDBY
  Hardware Severity:            0
```

Step 3 Verify the Last Running Config sync and Last Startup Config sync fields. They indicate the last time the running configuration and startup configuration were synchronized between the processor cards.

Step 4 Verify the active, standby, and Slot fields. They indicate in which slot the active processor card is configured.

Verifying Redundant Processor Card Functions

To troubleshoot the processor card function capabilities and redundancy, use the following commands:

Command	Purpose
show redundancy capability	Displays capabilities for the active and standby processor cards.
show redundancy clients	Displays internal redundancy software client information, which can be used to debug redundancy software.
show redundancy counters	Displays internal redundancy software counter information, which can be used to debug redundancy software.
show redundancy history	Displays the internal redundancy software history log, which can be useful for debugging redundancy software.
show redundancy running-config-file	Displays the running-config-file on the standby processor.
show redundancy states	Displays internal redundancy software state information.

Follow these steps to troubleshoot processor and redundancy capabilities on the system:

Step 1 Use the **show redundancy capability** command to display capabilities of the active or standby processor cards described in the "Verifying Hardware and Software Versions" section on page 6-8.

Step 2 Use the **show redundancy clients** command to display a list of internal redundancy clients.

```
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
```

Step 3 Use the **show redundancy counters** command to display internal redundancy software counters.

```
Switch# show redundancy counters
Redundancy Facility OMs
               comm link up = 0
        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 = 0
     tx buffers unavailable = 0
                buffers rx = 0
      buffer release errors = 0

 duplicate client registers = 0
  failed to register client = 0
       Invalid client syncs = 0
```

Step 4 Use the **show redundancy history** command to display internal redundancy software history.

```
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
```

Step 5 Use the **show redundancy running-config-file** command to display running configuration on the standby processor card.

```
sby-Switch# show redundancy running-config-file

Current configuration :601 bytes
!
version 12.1
no service pad
...
<Information deleted>
...
!
end
```

Step 6 Use the **show redundancy states** command to display internal redundancy software state information.

```
Switch# show redundancy states
       my state = 13 -ACTIVE
     peer state = 1  -DISABLED
           Mode = Simplex
           Unit = Primary
        Unit ID = 6
```

```
    Split Mode = Disabled
  Manual Swact = Disabled  Reason: Simplex mode
Communications = Down      Reason: Simplex mode

  client count = 4
client_notification_TMR = 30000 milliseconds
          RF debug mask = 0x80
```

Refer to the *Cisco ONS 15540 ESP Configuration Guide and Command Reference* for the following:

- Configuring processor card redundancy
- Upgrading the software image on the redundant processor card
- Downloading the IOS image on the processor cards

Checking the DDTs Database and Release Notes for Workarounds

There are two methods you can use to check for Cisco IOS software bugs (defect tracking tool numbers [DDTs]) in your version of the Cisco IOS software. You can use the Bug Navigator II or check the release notes. Often, your problems with the Cisco ONS 15540 have been fixed or a workaround has been determined in a more recent version of software.

Using Bug Navigator II

Bug Navigator II is a DDTS search tool you can use to search the DDTS database and ask either of two types of questions:

- Symptom Diagnostics (for example, “What defect is causing my current symptoms?”)
- Upgrade Planning (for example, “What software release is best for the features I am interested in?”)

To search the DDTS database, you can access Bug Navigator II on the World Wide Web at http://www.cisco.com/support/bugtools/bugtool.shtml. Then perform the following steps:

Step 1 Enter your user name and password at the login prompt if you are not already logged in to Cisco.com.

Step 2 Read the Bug Navigator II Help instructions.

Step 3 Select your hardware from the Cisco Hardware list. The Bug Navigator search tool replaces Bug Navigator II Help (in the right frame of the page).

Step 4 Select the following from the drop-down menus:

- Version
- Revision
- Severity

Note As an option, you can enter words or phrases (separated by commas) in the data entry field to limit your search.

Step 5 Click the Search button.

The entire window is replaced with a Bug Search Results window with a list of DDTs containing your search criteria. Look at the Bug reports listed in the titles column. An existing bug entry that describes the problem you are having may have been fixed in a more recent version of the Cisco IOS software. Look in the Fixed-in column for a later version of the Cisco IOS software. All you might have to do to solve your problem is upgrade your software.

If a software upgrade is not listed as a way to solve your problem, double-click on the bug title and read the DDTs details; a workaround might be listed there.

Checking Cisco IOS Release Notes

Release notes describe the features and caveats for Cisco IOS software releases. The release notes are listed by both product and Cisco IOS release number.

The “Caveats” section of the release notes lists known caveats by tracking the DDTs number and the release number, and indicates whether the caveat has been corrected.

The “Caveat Symptoms and Workarounds” section summarizes caveat symptoms and suggested workarounds. You can also search through this section online, using either a word string or the DDTs number.

Troubleshooting Performance History Counter Problems

This chapter describes how to troubleshoot performance history counter problems. This chapter contains the following sections:

- 7.1 Overview, page 7-1
- 7.2 Initial Troubleshooting Checklist, page 7-1
- 7.3 Interpreting Performance History Messages, page 7-2
- 7.4 Troubleshooting Performance History Counters, page 7-2

7.1 Overview

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

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

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

For more information on performance history counters, refer to the *Cisco ONS 15540 ESP Configuration Guide.*

7.2 Initial Troubleshooting Checklist

Follow this initial checklist before proceeding with the troubleshooting procedures:

- Issue the **show version** command to ensure that the IOS version is 12.2(29)SV or later.
- Issue **show interfaces** commands to ensure that the interface for which the performance history counters are being monitored is administratively up.
- Ensure that the encapsulation configured on the interface supports performance history counters.
- To preserve the performance history counters across a CPU switch module switchover, ensure that the `auto-sync counter interfaces` configuration is present in the running configuration.

7.3 Interpreting Performance History Messages

This section explains the informational messages that may be displayed on the command line interface (CLI) while you are working with the performance history counters.

Message	Description
Sorry! Current 15 minute interval [dec] on [interface] just started. Please try again.	This message indicates that the elapsed time and the valid time are equal to zero. This message is displayed if you issue the **show performance** command immediately after the current counter completes its 15 minute interval.
Sorry! No counters for this interface/encapsulation combination.	This message indicates that the encapsulation configured on the interface does not support performance history counters, or the monitoring of the transparent interfaces is disabled.
Sorry! No valid current 15 minute data for interval [dec] on [interface].	This message indicates that the specified interface was administratively down during the 15 minute interval of the current counter.
Sorry! No valid performance data for interval [dec] on [interface].	This message indicates that the specified interface was administratively down during the entire interval of the performance history counter.
Sorry! No valid 24 hour performance data for [interface].	This message indicates that the interface was administratively down during the full 24 hour interval of the 24-hour counter.
Sorry! 15 minute performance history register [dec] not available for [interface].	This message is displayed if the 15-minute history counter is yet to be created.
Sorry! 24 hour performance register not available for [interface].	This message is displayed if the 24-hour counter is yet to be created
Sorry! Current 15 minute register not available for [interface].	This message indicates that the specified interface does not support performance history counters.

7.4 Troubleshooting Performance History Counters

This section contains troubleshooting procedures for performance history counter problems.

7.4.1 Some Counters Are Not Displayed

Symptom Some interface counters are not displayed in the output of the **show performance** command.

Table 7-1 describes the potential causes of the symptom and the solutions.

Table 7-1 Some Counters Are Not Displayed

Possible Problem	Solution
Monitoring of the transparent interface of the transponder is disabled.	Issue the **monitor enable** command to enable monitoring of the transparent interface.
The missing interface counters are not supported by the performance history feature.	Refer to the *Cisco ONS 15540 ESP Configuration Guide* for the list of interface counters that are supported by the performance history feature.

7.4.2 Performance History Counters Are Not Preserved Across CPU Switch Module Switchovers

Symptom The performance history counters are not preserved across a CPU switch module switchover.

Table 7-2 describes the potential causes of the symptom and the solutions.

Table 7-2 Performance History Counters Are Not Preserved Across CPU Switch Module Switchovers

Possible Problem	Solution
Automatic synchronization of performance history counters is not enabled.	Issue the **auto-sync counter interfaces** command to enable the automatic syncing of the performance history counters to the standby CPU switch module.

Technical Support

When you have a problem that you cannot resolve, contact customer service. To help resolve these problems, gather relevant information about your network prior to calling. This appendix includes the following sections:

- Gathering Information About Your Internetwork, page A-1
- Providing Data to Customer Service, page A-2

Gathering Information About Your Internetwork

Before gathering any specific data, compile a list of all symptoms users have reported on the internetwork (such as connections dropping or slow host response).

The next step is to gather specific information. Typical information needed to troubleshoot internetworking problems fall into two general categories: information required for any situation and information specific to the topology, technology, protocol, or problem.

Information that is always required by technical support engineers includes the following:

- Configuration listing of all systems involved
- Complete specifications of all systems involved
- Version numbers of software (obtained by using the **show version** command) and Flash code (obtained by using the **show controllers** command) on all relevant systems
- Network topology map
- List of hosts and servers (host and server type, number on network, description of host operating systems that are implemented)
- List of network layer protocols, versions, and vendors

To assist you in gathering this required data, the **show tech-support** EXEC command has been added in Cisco IOS Release 11.1(4) and later. This command provides general information about the system that you can provide to your technical support representative when you are reporting a problem.

The **show tech-support** command display includes outputs from the **show version**, **show hardware**, **show diag power-on**, **show running-config**, **show controllers**, **show stacks**, **show interfaces**, **show buffers**, **show process memory**, and **show process** EXEC commands.

Specific information that might be needed by technical support varies, depending on the situation, and include the following:

- Output from the following general **show** commands:

show interfaces

show controllers [**atm** | **serial** | **e1** | **ethernet**]

show processes [**cpu** | **mem**]

show buffers

show memory summary

- Output from the following protocol-specific **show** commands:

  show *protocol* **route**

  show *protocol* **traffic**

  show *protocol* **interface**

  show *protocol* **arp**

- Output from relevant **debug** privileged EXEC commands
- Output from protocol-specific **ping** and **trace** command diagnostic tests, as applicable
- Network analyzer traces, as applicable
- Core dumps obtained by using the **exception dump** switch configuration command, or by using the **write core** switch configuration command if the system is operational, as appropriate

Getting the Data from Your System

When obtaining information from your system, tailor your method to the system that you are using to retrieve the information. Following are some hints for different platforms:

- PC and Macintosh—Connect a PC or Macintosh to the console port of the system and log all output to a disk file (using a terminal emulation program). The exact procedure varies depending on the communication package used with the system.
- Terminal connected to console port or remote terminal—The only way to get information with a terminal connected to the console port or with a remote terminal is to attach a printer to the Aux port on the terminal (if one exists) and to force all screen output to go to the printer. Using a terminal is undesirable because there is no way to capture the data to a file.
- UNIX workstation—At the UNIX prompt, enter the **script** *filename* command, then use Telnet to connect to the system. The UNIX **script** command captures all screen output to the specified filename. To stop capturing output and close the file, enter the end-of-file character (typically **^D**) for your UNIX system.

Note To get your system to automatically log specific error messages or operational information to a UNIX syslog server, use the **logging** *internet-address* switch configuration command. For more information about using the **logging** command and setting up a syslog server, refer to the Cisco IOS configuration guides and command reference publications.

Providing Data to Customer Service

If you need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact TAC (Cisco's Technical Assistance Center) to open a case. Contact TAC with a phone call or an e-mail message:

- North America: 800-553-2447, e-mail: tac@cisco.com
- Europe: 32 2 778 4242, e-mail: euro-tac@cisco.com
- Asia-Pacific: 61 2 9935 4107, e-mail: asiapac-tac@cisco.com

When submitting information to your technical support representative, electronic data is preferred. Electronic data significantly eases the transfer of information between technical support personnel and development staff. Common electronic formats include data sent via e-mail and files sent using FTP (File Transfer Protocol).

If you are submitting data to your technical support representative, use the following list to determine the preferred method for submission:

1. The preferred method of information submission is through FTP service over the Internet. If your environment supports FTP, you can place your file in the incoming directory on the host cco.cisco.com.
2. The next best method is to send data by electronic mail. Before using this method, be sure to contact your technical support representative, especially when transferring binary core dumps or other large files.

   If you use e-mail, do not use encoding methods such as binhex or zip. Only MIME-compliant mail should be used.
3. Use a PC-based communications protocol, such as Kermit, to upload files to Cisco.com. Again, be sure to contact your technical support representative before attempting any transfer.
4. Transfer by disk or tape.
5. The least favorable method is hard-copy transfer by fax or physical mail.

INDEX

A

accessibility tests
  online diagnostics **1-8**
APS
  debugging **2-4**
  description **2-2**
  displaying configurations **2-2 to 2-4**
  troubleshooting **2-2**
Automatic Protection Switching. See APS

B

booting
  redundant processor cards **6-13**
Bug Navigator II
  searching DDT database **6-17**

C

Cisco.com
  uploading files to **A-3**
Cisco TAC. See TAC
client side interfaces
  debugging **3-5**
  troubleshooting **3-1**
commands **1-6**
configuring
  online diagnostic tests **1-8 to 1-9**
connectivity. See network connectivity
customer service and support. See TAC

D

DDTSs
  using Bug Navigator II **6-17**
debug aps command **2-4, 3-5**
debug cdp command **3-5**
debug commands
  cautions **1-6**
  disabling **1-6**
  troubleshooting client side interfaces **3-5**
  troubleshooting trunk side interfaces **4-7**
  using **1-6**
debug diag online command **1-8**
debug lcmdc command **3-5**
debug oscp command **3-5**
debug ports command **3-5**
debug ports wave command **4-7**
debug ports wdm command **4-7**
defect tracking tool. See DDT
Device Fault Manager. See DFM
DFM
  description **1-4**
diagnostic commands
  description **1-5**
  types **1-5 to 1-7**
diag online command **1-8**
diag online oir command **1-8**
documentation
  related **xii**

E

echo messages. See ICMP echo messages

error message logging. See message logging

F

FTP
  sending data to TAC **A-3**

H

hardware
  troubleshooting **1-3**
  verifying versions **6-8 to 6-10**
hubbed ring topologies
  line card protection example (figure) **5-15**
  splitter protection example (figure) **5-12**
  troubleshooting line card protection **5-14 to 5-17**
  troubleshooting splitter protection **5-11 to 5-14**

I

ICMP echo messages **1-7**
interfaces
  troubleshooting connections (figure) **5-2**
Internet Control Message Protocol echo messages. See ICMP echo messages
internetwork maps. See network maps **1-3**
IOS images. See system images **6-18**

K

Kermit protocol
  providing data to TAC **A-3**

L

line card protection
  troubleshooting hubbed ring topologies **5-14 to 5-17**
  troubleshooting meshed ring topologies **5-20 to 5-23**
  troubleshooting point-to-point topologies **5-9 to 5-11**
logging command **A-2**
loopback tests
  description **5-1**

M

Macintosh
  logging system output **A-2**
manual switchovers. See switchovers
memory
  troubleshooting processor card **6-7**
meshed ring topologies
  example (figure) **5-21**
  line card protection example (figure) **5-21**
  splitter protection example (figure) **5-18**
  troubleshooting line card protection **5-20 to 5-22**
  troubleshooting splitter protection **5-17 to 5-20**
message logging
  choosing destinations **A-2**
  syslog servers **A-2**
monitoring. See network monitoring **1-4**

N

network connectivity
  checking **3-3**
network evaluation
  before troubleshooting **2-1**
network management
  tools supported **1-3**
network management Ethernet ports. See NME
network maps
  preparing for failures **1-3**
network monitoring
  CiscoView **1-4**
network performance
  debug commands (caution) **1-6, 2-4, 4-7**
NME

displaying interface configurations **6-5**
troubleshooting connections **6-5**
no debug all command **1-6**
no debug command **1-6**

O

OIR tests
description **1-8**
online diagnostics
configuring **1-7 to 1-9**
displaying configuration **1-9 to 1-11**
optical supervisory channel. See OSC
Optical Supervisory Channel Protocol. See OSCP
OSC
description **2-5**
OSCP
troubleshooting connections **4-5 to 4-7**

P

passwords
recovering **6-4 to 6-5**
PCs
logging system output **A-2**
performance. See network performance
performance history counters
description **7-1**
interpreting messages **7-2**
not preserved across CPU switchovers **7-3**
some counters are not created **7-2**
troubleshooting checklist **7-1**
ping command
checking connectivity **1-7**
checking optical network **5-2 to 5-22**
point-to-point topologies
troubleshooting line card protection **5-9 to 5-11**
troubleshooting splitter protection **5-7 to 5-9**
troubleshooting without protection **5-5 to 5-7**
problem solving
steps **1-2**
troubleshooting models (figure) **1-1**
processor cards
displaying configuration **6-1**
software compatibility **6-10**
troubleshooting connections **6-5**
troubleshooting memory **6-7**
troubleshooting redundant **6-13**
verifying hardware versions **6-8**
verifying software versions **6-8**

R

recovering
passwords **6-4**
redundancy
troubleshooting processor cards **6-13 to 6-17**
release notes
checking for workarounds **6-18**
remote terminals
logging system output **A-2**

S

script command (UNIX) **A-2**
security
password recovery **6-4 to 6-5**
servers
syslog **A-2**
show aps group command **2-3**
show aps interface command **2-3**
show aps summary command **2-1, 2-3**
show buffers command **1-6, 6-8**
show command **1-5**
show connect command **2-1, 3-3, 4-5**
show controllers command **1-6**

show controllers FastEthernet 0 command **6-5**
show flash command **1-6**
show hardware command **6-8**
show interfaces command **1-6**
show interfaces FastEthernet 0 command **6-5**
show interfaces thru command **4-1**
show interfaces transparent command
  client side checking **3-1**
show interfaces wave 0 command **4-2**
show interfaces wave command
  trunk side checking **4-1, 5-2**
show interfaces wavepatch command **4-1**
show interfaces wdm command **4-2**
show memory command **1-6, 6-8**
show oscp info command **4-5**
show oscp interface command **4-5**
show oscp neighbor command **4-5**
show oscp statistics command **4-5**
show oscp traffic command **4-5**
show processes command **1-6**
show redundancy capability command **6-10, 6-15**
show redundancy clients command **6-15**
show redundancy command **6-13**
show redundancy counters command **6-15**
show redundancy history command **6-15**
show redundancy running-config-file command **6-15**
show redundancy states command **6-15**
show running-config command **1-6, 6-2**
show stacks command **1-6**
show startup-config command **1-6**
show tech-support command **A-1**
show topology command **3-3**
show version command **1-6, 6-7**
software
  checking for workarounds **6-17**
  compatibility **6-10**
  downloading from Cisco.com **6-17**
  verifying versions **6-8**
splitter protection
  troubleshooting hubbed ring topologies **5-11 to 5-14**
  troubleshooting meshed ring topologies **5-17 to 5-20**
  troubleshooting point-to-point topologies **5-7 to 5-9**
support, technical. See TAC
switchovers
  forcing manual **2-4**
syslog servers
  logging troubleshooting information **A-2**
system images
  checking release notes **6-17**

T

TAC
  contacting **A-2**
  gathering data for **A-1 to A-2**
  providing data to **A-3**
  show tech-support command **A-1**
Technical Assistance Center. See TAC
technical support. See TAC
terminals. See remote terminals
thru interfaces
  displaying configurations **4-3**
traceroute command **1-7**
transparent interfaces
  basic checks **4-1**
  checking configuration **3-1**
  checks **3-1**
  troubleshooting **3-1 to 3-5**
troubleshooting **5-20**
  problem-solving models (figure) **1-1**
  problem-solving steps **1-2**
  tools **1-4 to 1-5**
  using internetwork maps **1-3**
trunk side interfaces
  debugging **4-7**
  troubleshooting **4-1 to 4-7**

U

UNIX
  logging system output **A-2**
  script command **A-2**
unprotected topologies. See point-to-point topologies

W

wave interfaces
  displaying configurations **5-3**
wavepatch interfaces
  displaying configurations **4-3**
workarounds
  checking release notes **6-17**