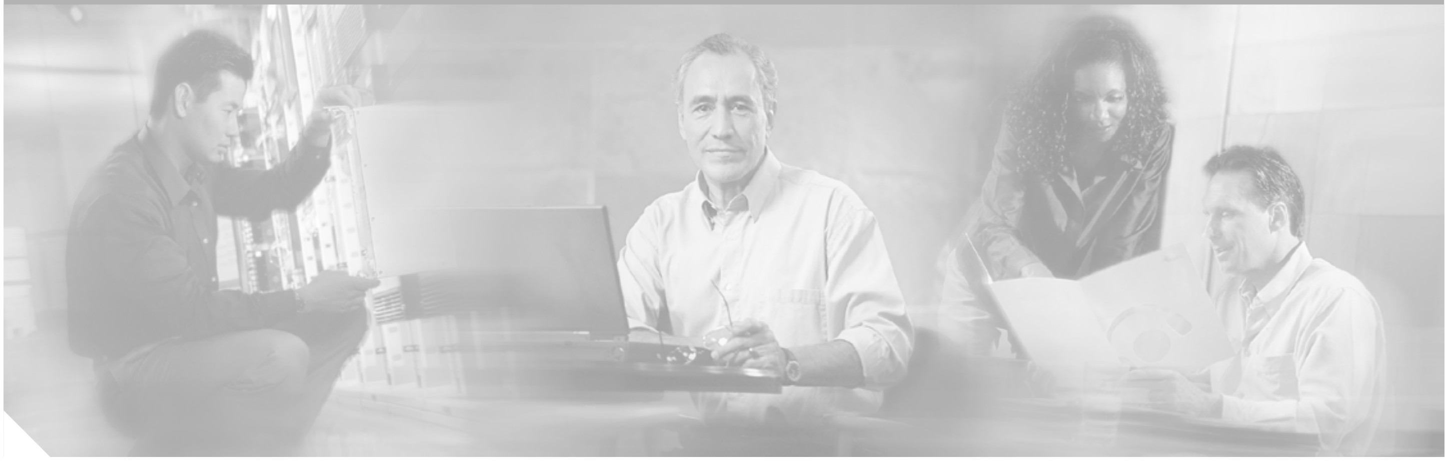
Cisco Systems



Cisco MPLS Diagnostics Expert 1.0 User Guide on ISC 4.1

December 12, 2005

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

Customer Order Number:
Text Part Number: OL-7645-01

Cisco MPLS Diagnostics Expert 1.0 User Guide on ISC 4.1

CONTENTS

About This Guide v

Audience v

Organization v

Related Documentation vi

Technology-Related Documentation vii

Obtaining Documentation vii

Cisco.com vii

Product Documentation DVD vii

Ordering Documentation viii

Documentation Feedback viii

Cisco Product Security Overview viii

Reporting Security Problems in Cisco Products ix

Obtaining Technical Assistance ix

Cisco Technical Support & Documentation Website ix

Submitting a Service Request x

Definitions of Service Request Severity x

Obtaining Additional Publications and Information xi

CHAPTER 1 Introduction 1-1

1.1 Cisco MPLS Diagnostics Expert Overview 1-1

1.2 Prerequisite Knowledge 1-2

1.3 Supported Hardware and IOS Versions 1-3

1.4 MPLS Diagnostics Expert Features 1-4

CHAPTER 2 Getting Started 2-1

2.1 Installing Cisco MPLS Diagnostics Expert 2-2

2.2 Licensing 2-3

2.3 User Roles 2-3

2.4 Network Configuration 2-3

2.5 Inventory Setup 2-4

2.5.1 Manual Creation 2-5

2.5.2 Discovery 2-5

2.5.3 Inventory Manager Device Import 2-6

2.5.4 ISC APIs 2-7

2.5.5 Device Configuration Collection 2-7

2.5.5.1 Synchronizing the ISC Repository with Device Configuration 2-7

CHAPTER 3 Using Cisco MPLS Diagnostics Expert 3-1

3.1 Performing an MPLS VPN Connectivity Verification Test 3-2

3.1.1 Configuration Using Customer VPN Information 3-8

3.1.2 VPN Topologies 3-10

3.1.2.1 Testing with Hub and Spoke VPN Topology 3-10

3.1.2.2 Testing with Intranet/Extranet VPN Topology 3-14

3.1.2.3 Testing with Central Services VPN Topology 3-14

3.1.3 Progress Window 3-14

3.2 Interpreting the Test Results 3-16

3.2.1 Data Path 3-17

3.2.1.1 Device Actions 3-18

3.2.2 Test Details 3-19

3.2.3 Test Log 3-21

3.2.4 Export 3-22

3.3 Advanced Troubleshooting Options 3-22

3.3.1 Reverse Path Testing 3-23

3.3.2 MTU Analysis 3-23

3.3.3 LSP Visualization 3-24

3.3.4 LSP Troubleshooting 3-25

CHAPTER 4 How Does Cisco MPLS Diagnostics Expert Work? 4-1

APPENDIX A Frequently Asked Questions A-1

APPENDIX B Unsupported Scenarios B-1

B.1 IP Unnumbered Interfaces B-1

B.2 Common PE for Local and Remote Sites B-1

B.3 Core Tunneling Protocols B-1

B.4 Multicast VPN B-2

B.5 Channelized Interfaces B-2

INDEX

About This Guide

This guide describes how to use the Cisco MPLS Diagnostics Expert application for the Cisco IP Solution Center (ISC) Release 4.1.

This preface defines the following:

- Audience, page v
- Organization, page v
- Related Documentation, page vi
- Obtaining Documentation, page vii
- Documentation Feedback, page viii
- Cisco Product Security Overview, page viii
- Obtaining Technical Assistance, page ix
- Obtaining Additional Publications and Information, page xi

Audience

This guide is designed for network managers and operators who are responsible for deploying, managing, and troubleshooting MPLS VPNs within your network. The network manager and operators should be familiar with the following topics:

- Basic concepts and terminology used in internetworking
- MPLS terms and technology
- Network topologies and protocols

Organization

This guide contains the following chapters and appendices:

- Chapter 1, "Introduction"
- Chapter 2, "Getting Started"
- Chapter 3, "Using Cisco MPLS Diagnostics Expert"
- Chapter 4, "How Does Cisco MPLS Diagnostics Expert Work?"

- Appendix A, “Frequently Asked Questions”
- Appendix B, “Unsupported Scenarios”

Related Documentation

The entire documentation set for Cisco IP Solution Center, 4.1 can be accessed at:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1

The following documents comprise the ISC 4.1 documentation set.

General documentation (in suggested reading order):

- Cisco IP Solution Center Getting Started and Documentation Guide, 4.1
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/docguide/index.htm
- Release Notes for Cisco IP Solution Center, 4.1
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/relnotes/index.htm
- Cisco IP Solution Center Installation Guide, 4.1
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/install/index.htm
- Cisco IP Solution Center Infrastructure Reference, 4.1
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/infrastr/index.htm
- Cisco IP Solution Center System Error Messages, 4.1
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/mess/index.htm

Application and technology documentation (listed alphabetically):

- Cisco IP Solution Center L2VPN User Guide, 4.1
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/l2vpn/index.htm
- Cisco IP Solution Center MPLS VPN User Guide, 4.1
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/mpls/index.htm
- Cisco IP Solution Center Quality of Service User Guide, 4.1
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/qos/index.htm
- Cisco IP Solution Center Traffic Engineering Management User Guide, 4.1
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/tem/index.htm
- Cisco MPLS Diagnostics Expert 1.0 User Guide on ISC 4.1
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/trble/index.htm

API Documentation:

- *Cisco IP Solution Center API Programmer Guide, 4.1*
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/api_set/api_gd/index.htm
- Index: *Cisco IP Solution Center API Programmer Reference, 4.1*
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/api_set/api_ref/index.htm

Note All documentation *might* be upgraded over time. All upgraded documentation will be available at the same URLs specified in this document.

Technology-Related Documentation

- Cisco MPLS Embedded Management web page

  http://www.cisco.com/en/US/partner/tech/tk436/tk892/tech_brief09186a00801f4a8d.html
- Cisco Multiprotocol Label Switching Management Strategy

  http://www.cisco.com/en/US/tech/tk436/tk892/tech_brief0900aecd800f6e31.html
- Cisco MPLS Embedded Management Q&A

  http://www.cisco.com/en/US/partner/tech/tk436/tk892/technologies_q_and_a_item09186a00801f4a62.shtml

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

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same 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=) from Cisco Marketplace at this URL:

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

Ordering Documentation

Beginning June 30, 2005, 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 send comments about Cisco documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

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 can perform these tasks:

- 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 and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from 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 might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—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.

- 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 to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*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.

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)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

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

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

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

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, 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

CHAPTER 1

Introduction

This chapter provides an overview of the Cisco MPLS Diagnostics Expert application.

This chapter contains the following sections:

- 1.1 Cisco MPLS Diagnostics Expert Overview, page 1-1
- 1.2 Prerequisite Knowledge, page 1-2
- 1.3 Supported Hardware and IOS Versions, page 1-3
- 1.4 MPLS Diagnostics Expert Features, page 1-4

1.1 Cisco MPLS Diagnostics Expert Overview

The Cisco MPLS Diagnostics Expert application is designed for network operations center (NOC) fault and assurance operators. It provides automated troubleshooting and diagnostics for access circuits, edge, and core failures in Layer 3 Multiprotocol Label Switching (MPLS) VPN deployments.

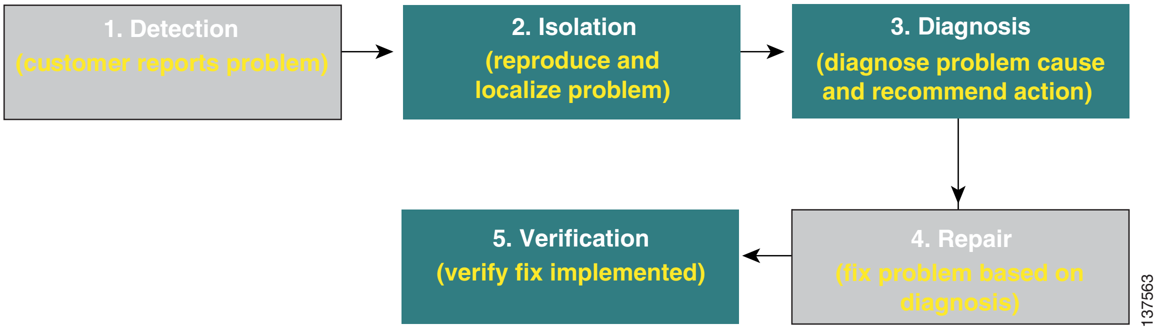
Cisco MPLS Diagnostics Expert significantly reduces the time to isolate and diagnose failures in these networks by employing an automated, workflow-based troubleshooting approach. This workflow-based troubleshooting uses a Cisco-unique MPLS VPN Failures Knowledge Base to diagnose failure conditions and provide intelligent recommendations of potential causes of failure. Cisco MPLS Diagnostics Expert can be used as a standalone application by customers who do not use any of the ISC product family applications, or it can be used alongside the other ISC product family applications. ISC MPLS VPN provisioning is not mandatory for use of the Cisco MPLS Diagnostics Expert. Cisco MPLS Diagnostics Expert is the latest addition to the ISC product family.

In effective fault finding and troubleshooting, there are five steps:

1. Detection
2. Isolation
3. Diagnosis
4. Repair
5. Verification

This release of the Cisco MPLS Diagnostics Expert is designed to support reactive situations in which an end customer reports a problem with their VPN service. This is essentially the Detection step in Figure 1-1. The Repair function is also not supported because many providers prefer to be in complete control of any changes made to router devices and might have specific in-house procedures for doing so.

Figure 1-1 The Reactive Fault Lifecycle


1. Detection
(customer reports problem)
2. Isolation
(reproduce and localize problem)
3. Diagnosis
(diagnose problem cause and recommend action)
4. Repair
(fix problem based on diagnosis)
5. Verification
(verify fix implemented)
137563

Note Steps 2, 3, and 5 are performed by Cisco MPLS Diagnostics Expert. Steps 1 and 4 must be performed manually.

Cisco MPLS Diagnostics Expert focuses on the Isolation, Diagnosis, and Verification steps. It provides invaluable functionality for isolating and diagnosing failures in the network, determining the device(s) at fault, and checking appropriate device status and configuration to determine the likely reason for the failure. Cisco MPLS Diagnostics Expert also provides the ability to re-run tests to verify that changes made to the device configuration have resolved the issue.

The functionality can be used on its own, without any dependency on any other modules in ISC (for example, VPN provisioning or Traffic Engineering Management). It can also be used in ISC installations where some or all of the other ISC modules are used. If the MPLS VPN Provisioning functionality is used, then Customer and VPN data can be used as a starting point for troubleshooting, in order to locate the endpoints (Customer Edge devices) between which connectivity is tested.

In addition to troubleshooting, Cisco MPLS Diagnostics Expert can also be used for VPN post-provisioning checks. After deploying a VPN, either manually or using ISC VPN provisioning, a connectivity test can be run to verify that the VPN has been provisioned successfully.

1.2 Prerequisite Knowledge

Cisco MPLS Diagnostics Expert has been designed for use by users who have minimal MPLS VPN knowledge. However, due to the complex nature of MPLS VPNs, it is recommended that you will gain maximum advantage from Cisco MPLS Diagnostics Expert if you are familiar with MPLS VPNs, in accordance with RFC 2547. In particular, knowledge of RFC 2547 architecture, topology, control, and data planes is helpful to understand how to best use the application and interpret the results.

A Cisco MPLS Diagnostics Expert MPLS VPN Connectivity Verification Test can be performed by a user with little or no MPLS VPN knowledge, and, where necessary, the test results can be exported for interpretation by an engineer familiar with MPLS VPNs.

Recommended reading:

- MPLS and VPN Architectures: Ivan Pepelnjak, Jim Guichard, Cisco Press
- Troubleshooting Virtual Private Networks: Mark Lewis, Cisco Press
- RFC 2547: http://www.ietf.org/rfc/rfc2547.txt?number=2547

1.3 Supported Hardware and IOS Versions

For details of Provider (P) and Provider Edge (PE) device types and IOS versions supported by Cisco MPLS Diagnostics Expert 1.0 for ISC 4.1, see *Cisco IP Solution Center Installation Guide, 4.1*.

Note Support for additional device types and IOS versions could be added in patch releases. For details of the latest patch releases and the supported device types and IOS versions see Cisco.com.

The device types and IOS versions detailed in the *Cisco IP Solution Center Installation Guide, 4.1* support the MPLS label switched path (LSP) Ping and Traceroute feature. This feature is required for MPLS Diagnostics Expert troubleshooting. If all P and PE devices comply with the list of supported device types and IOS versions, Cisco MPLS Diagnostics Expert can troubleshoot access circuit, MPLS VPN, and MPLS core problems. Cisco MPLS Diagnostics Expert is tolerant to other device types and IOS versions, including other vendors equipment. However, when the network includes P or PE devices that do not comply with this list, a complete diagnosis might not be possible. Table 1-1 shows the possible scenarios and likely outcome.

Table 1-1 Hardware and IOS Version Compliance

Scenario	Outcome
All P and PE devices comply with the supported Cisco hardware and IOS versions.	MPLS VPN Connectivity Verification test successfully troubleshoots access circuit, MPLS VPN, and MPLS core issues.
All PE devices comply with the supported Cisco hardware and IOS versions. One or more P device(s) do not comply with the supported Cisco hardware and IOS versions, including other vendors equipment.	MPLS VPN Connectivity Verification test successfully troubleshoots access circuit and MPLS VPN issues, but might be unable to complete troubleshooting of MPLS core issues.
PE device(s) do not comply with the supported Cisco hardware and IOS versions, including other vendors equipment.	MPLS VPN Connectivity Verification test cannot be run.

Cisco MPLS Diagnostics Expert supports both managed and unmanaged CE routers from any vendor. There are no device type or IOS version requirements for CE devices.

Cisco MPLS Diagnostics Expert can work with other device types and IOS versions that support the MPLS LSP Ping and Traceroute feature. Use the Cisco Feature Navigator for details of device types and IOS versions that support this feature see, http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

Note MPLS Diagnostics Expert is supported only for the device types and IOS version detailed above. Additional device types and IOS versions are not supported.

1.4 MPLS Diagnostics Expert Features

MPLS Diagnostics Expert troubleshooting and diagnostics supports the following three domains:

- Access Circuit
- MPLS Core
- Layer 3 VPN

Access circuit troubleshooting includes basic layer 1 and layer 3 troubleshooting and advanced layer 2 troubleshooting for ATM, Frame Relay, and Ethernet.

MPLS core troubleshooting supports data plane, and control plane diagnostics. This is provided for all MPLS core and edge devices running a Cisco IOS version with MPLS Operation, Administration, and Maintenance (OAM) support. For details of Cisco IOS versions with MPLS OAM support see 1.3 Supported Hardware and IOS Versions, page 1-3.

Layer 3 VPN troubleshooting supports MPLS/MP-BGP VPNs based on RFC2547. The following topologies are supported: hub and spoke, central services, full mesh, and intranet/extranet VPN.

MPLS Diagnostics Expert does not troubleshoot routing protocols, IP connectivity within the core, inter-Autonomous Systems (AS), Carrier-Supporting-Carrier or traffic engineered MPLS cores. For further details of unsupported scenarios see Appendix B, “Unsupported Scenarios”.

Getting Started

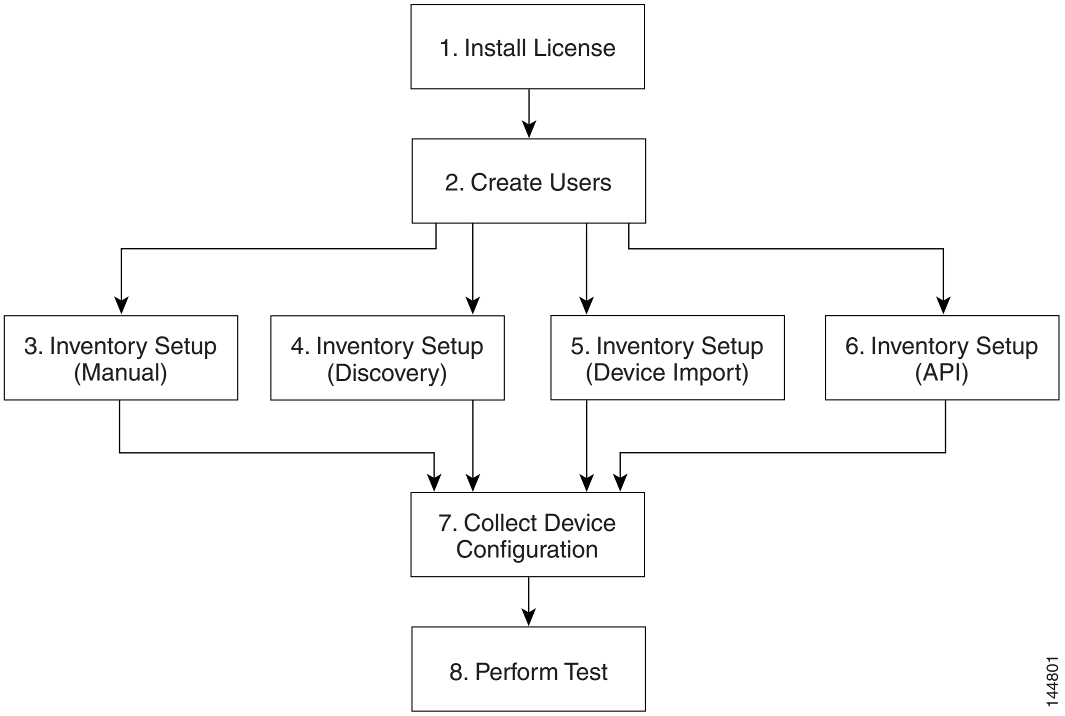
This chapter describes how to get started using Cisco MPLS Diagnostics Expert.

This chapter contains the following sections:

- 2.1 Installing Cisco MPLS Diagnostics Expert, page 2-2
- 2.2 Licensing, page 2-3
- 2.3 User Roles, page 2-3
- 2.4 Network Configuration, page 2-3
- 2.5 Inventory Setup, page 2-4

Figure 2-1 describes the getting started workflow for Cisco MPLS Diagnostics Expert. This workflow assumes that you have already installed ISC as described in the *Cisco IP Solution Center Installation Guide, 4.1*.

Figure 2-1 Getting Started Workflow


1. Install License
2. Create Users
3. Inventory Setup (Manual)
4. Inventory Setup (Discovery)
5. Inventory Setup (Device Import)
6. Inventory Setup (API)
7. Collect Device Configuration
8. Perform Test
144801

1. Install License—Install MPLS Diagnostics Expert license key. See 2.2 Licensing, page 2-3.
2. Create Users—Create users and assign MPLS Diagnostics Expert user role. See 2.3 User Roles, page 2-3.
3. Inventory Setup (Manual)—Manually create required ISC inventory objects. See 2.5 Inventory Setup, page 2-4.
4. Inventory Setup (Discovery)—Create required ISC inventory objects using ISC Discovery. See 2.5 Inventory Setup, page 2-4.
5. Inventory Setup (Device Import)—Create required ISC inventory objects using Inventory Manager Import Devices feature. See 2.5 Inventory Setup, page 2-4.
6. Inventory Setup (API)—Create required inventory objects through ISC APIs. See 2.5 Inventory Setup, page 2-4.
7. Collect Device Configuration—Collect device configuration, including interface configuration, and add to ISC inventory. A scheduled task can be setup to periodically synchronize ISC inventory with actual device configuration. See 2.5.5 Device Configuration Collection, page 2-7.
8. Perform Test—Configure and run an MPLS VPN Connectivity Verification test. See 3.1 Performing an MPLS VPN Connectivity Verification Test, page 3-2.

2.1 Installing Cisco MPLS Diagnostics Expert

Cisco MPLS Diagnostics Expert is installed as part of the standard ISC installation. It must then be activated by installing a Cisco MPLS Diagnostics Expert license. For detailed instructions of how to install Cisco MPLS Diagnostics Expert, see *Cisco IP Solution Center Installation Guide, 4.1*.

2.2 Licensing

The Cisco MPLS Diagnostics Expert product requires a separate license key. The license key is provided with the ISC installation CD-ROM. Upgrade licenses for further attachment circuits can be purchased from Cisco.com.

Cisco MPLS Diagnostics Expert licensing is implemented using the standard ISC licensing mechanism. For detailed instructions of how to install the Cisco MPLS Diagnostics Expert license key see the Administration chapter in *Cisco IP Solution Center Infrastructure Reference, 4.1*.

Note If a valid license key has not been installed, the Diagnostics tab does not appear within ISC, and you are unable to invoke any Cisco MPLS Diagnostics Expert functionality.

2.3 User Roles

The functionality available to you as an ISC user is determined by your assigned user roles. To use the Cisco MPLS Diagnostics Expert functionality, you must be assigned the *MPLSDiagnosticsRole*. This user role also allows you to create and delete devices, collect device configuration, and to perform an MPLS VPN Connectivity Verification test.

By default, all users with the *MPLSDiagnosticsRole* user role have the ability to invoke device actions, such as, Telnet, for devices displayed in the Data Path on the Test Result window. The functionality can be disabled on a per-user basis. To disable this functionality you must create a new user role. This new user role must then be assigned to users for which device actions are not desired and the pre-defined *MPLSDiagnosticsRole* should be removed.

The new user role should be identical to the *MPLSDiagnosticsRole*, except that it should not have the *MPLS Diagnostics Console Access resource*. To create this new role, you should copy the *MPLSDiagnosticsRole*, remove the MPLS Diagnostics Console Access resource, and assign a name to the new role.

See the Administration chapter in *Cisco IP Solution Center Infrastructure Reference, 4.1* for detailed instructions of how to:

- create ISC users and user roles, including assigning user roles
- create a new user role by copying an existing user role

2.4 Network Configuration

MPLS IP Time To Live (TTL) propagation is enabled by default on Cisco devices. MPLS Diagnostics Expert requires that MPLS IP TTL propagation is enabled within the MPLS core. If MPLS IP TTL propagation is not enabled, then MPLS Diagnostics Expert is unable to troubleshoot problems within the MPLS core. Troubleshooting of problems in the access circuit, or on the edge of the MPLS core is still possible.

To disable MPLS IP TTL propagation for packets forwarded into the MPLS core use the **no mpls ttl-propagate forward** IOS command. This command stops TTL propagation for packets forwarded into the MPLS core, but allows TTL propagation for packets sent from within the MPLS core. Cisco MPLS Diagnostics Expert functions correctly in this situation.

When TTL propagation is disabled using the command **no mpls ip propagate-ttl**, then all TTL propagation is disabled and MPLS Diagnostics Expert is unable to troubleshoot your MPLS network.

2.5 Inventory Setup

Cisco MPLS Diagnostics Expert can be used without any dependency on other ISC modules. However, before it can be used, the ISC repository must be populated with a number of objects. As a minimum this includes Provider, Provider Region, Device, and PE Device objects. The role of each of these objects is explained below:

- Provider—A Provider is typically a service provider or large corporation that provides network services to a customer. A Provider is a logical inventory object that represents a particular provider.
- Provider Region—A Provider Region is considered to be a group of provider edge routers (PEs) within a single Border Gateway Protocol (BGP) autonomous system. The primary objective for defining Provider Regions is to allow a provider to employ unique IP address pools in large Regions, such as Europe, Asia Pacific, and so forth.
- Device—A Device in ISC is a logical representation of a physical device in the network. Every network element that ISC manages must be defined as a device in the system.
- PE Device—A PE Device is a logical representation of a Provider Edge (PE) or Provider (P) router that has been associated with a particular Provider Region. A PE Device must first be added as a Device.

All Provider Edge (PE) and Provider (P) routers in the MPLS network must be added to the ISC inventory. Each Provider Edge router should be created as a Device and then as a PE Device with a Role Type of N-PE (Network-facing PE). Each Provider device should be created as a Device and then as a PE Device with a role type of P (Provider). Adding customer premises equipment (CPE) devices to the ISC inventory is optional.

Note Where a Device is acting as both a Provider and Provider Edge Device it should be created as a PE Device with a Role Type of N-PE (Network-facing PE).

Many MPLS VPN networks employ a Route Reflector. It is recommended that Route Reflectors should be added to the ISC inventory. A Route Reflector should be added as a Device and then as a PE Device with role type of P (Provider). By adding the Route Reflector to the ISC inventory, Cisco MPLS Diagnostics Expert is able to identify possible failures involving this device.

Note If other ISC features are being used to manage the MPLS network, many of the required inventory objects might already exist. For example, if the ISC MPLS VPN feature is being used, the required Provider, Provider Region, and Provider Edge devices might already exist. In this case only the Provider devices must be added.

A number of options exist for creating the required inventory objects. These objects can be created manually through the ISC GUI, using the ISC Discovery functionality, using the Inventory Manager Import Devices functionality, or using third-party Operations Support System (OSS) client programs that utilize the ISC APIs. Each of these options is described in the following sections:

- 2.5.1 Manual Creation, page 2-5
- 2.5.2 Discovery, page 2-5

- 2.5.4 ISC APIs, page 2-7
- 2.5.5 Device Configuration Collection, page 2-7

Note When creating Devices, the Device access information (login and passwords) must match that configured on the physical device.

2.5.1 Manual Creation

Manual creation allows you to add objects to the ISC Repository by entering the required configuration through the ISC Graphical User Interface (GUI). Manual object creation is recommended where a small number of objects are being added to the ISC Repository. The sequence for manual object creation is shown below:

1. Create Provider
2. Create Provider Region
3. Create Devices
4. Collect Device configuration, including interface configuration
5. Create PE Devices, including assigning roles for Provider and Provider Edge devices

Note Both Provider (P) and Provider Edge (PE) devices should be added to the ISC repository as PE Device objects with an appropriate PE Role Type. For details of the PE Role Types that should be assigned to Provider and Provider Edge devices, see, *Cisco IP Solution Center Infrastructure Reference, 4.1*.

For details of how to manually create Provider, Provider Region, Device and PE Device objects, see *Cisco IP Solution Center Infrastructure Reference, 4.1* (**Service Inventory > Inventory and Connection Manager**.)

When manually creating Devices, you must also add the interface configuration for these devices.

Interface configuration can either be added manually during Device creation, or by using a Task Manager Collect Configuration task. For details of how to perform a Task Manager Collect Configuration task see, 2.5.5 Device Configuration Collection, page 2-7. We recommend that you use a Collect Configuration task.

2.5.2 Discovery

Discovery allows you to add the devices in your network to the ISC Repository by configuring minimal device and topology information in XML files. The Discovery process then queries these devices and populates the ISC Repository with the required device and topology information. We recommend that Discovery is used where a large number of objects are being added to the Repository. For details of how to discover devices see *Cisco IP Solution Center Infrastructure Reference, 4.1* (**Service Inventory > Discovery**).

When discovering devices for Cisco MPLS Diagnostics Expert you should perform an MPLS VPN discovery using the Device/Topology method. CDP Discovery should not be used for discovery of MPLS VPNs.

Before running Discovery it is necessary to create the required Discovery configuration files, see *Cisco IP Solution Center Infrastructure Reference, 4.1* (**Service Inventory > Discovery**).

Warning **Running Discovery overwrites the existing ISC Repository. If you plan to use Discovery do not create any inventory objects or add any configuration to the Repository before running Discovery.**

Note It is currently only possible to run Discovery once. Any devices that require to be added after Discovery has been run must be added using another method.

Note When adding devices to the ISC Repository both Provider (P) and Provider Edge (PE) devices should be added as PE Device objects, with an appropriate PE Role Type. For details of the PE Role Types that should be assigned to Provider Edge and Provider devices see, *Cisco IP Solution Center Infrastructure Reference, 4.1*.

Note After Discovery has completed, you must run a Task Manager Collect Configuration task for all discovered devices. If you do not run a Collect Configuration task Cisco MPLS Diagnostics Expert is unable to log in to the discovered devices to perform troubleshooting. For details of how to perform a Task Manager Collect Configuration task see, 2.5.5 Device Configuration Collection, page 2-7.

2.5.3 Inventory Manager Device Import

The Inventory Manager Import Devices feature allows you to import multiple devices into the ISC Repository from files containing the Cisco IOS running configuration of the devices. We recommend that the Inventory Manager Import Devices feature is used where a large number of objects are being added to the Repository. For details of how to import devices, see *Cisco IP Solution Center Infrastructure Reference, 4.1* (**Service Inventory > Inventory and Connection Manager > Inventory Manager**.)

Before importing Provider (P) and Provider Edge (PE) devices you must create the required Provider and Provider Region objects. For details of how to manually create Provider and Provider Region objects, see *Cisco IP Solution Center Infrastructure Reference, 4.1* (**Service Inventory > Inventory and Connection Manager**.)

When importing devices you must specify the directory where files containing the Cisco IOS running configuration are located. Do not specify the file names. The files must be located in a file system directory accessible from the ISC server.

Note Both Provider (P) and Provider Edge (PE) devices are added to the ISC Repository as PE Devices with an appropriate PE Role Type. While importing devices, remember to assign the correct PE Role Type for PE and P devices. For details of the role types that should be assigned to Provider and Provider Edge devices, see *Cisco IP Solution Center Infrastructure Reference, 4.1*.

Note The enable secret password is encrypted before it is added to the Cisco IOS running configuration. As a result, the Device Import feature is unable to set the enable secret password for devices imported into the ISC Repository. If the enable secret password is set on any devices being imported, you must manually configure the enable password for these devices in the ISC Repository. If both the enable and enable secret passwords are set for a device, the Inventory Manager Import Devices feature will use the enable password for the device added to the ISC Repository. You must override this password with the correct enable secret password. The enable password for devices in the ISC Repository can be set during or after device import.

Note After Device Import has completed, you must run a Task Manager Collect Configuration task for all imported devices. If you do not run a Collect Configuration task Cisco MPLS Diagnostics Expert will be unable to log in to the imported devices to perform troubleshooting. For details of how to perform a Task Manager Collect Configuration task, see 2.5.5 Device Configuration Collection, page 2-7.

2.5.4 ISC APIs

The Cisco IP Solution Center (ISC) application program interface (API) allows you to use operations support system (OSS) client programs to connect to the ISC system. The ISC APIs provide a mechanism for inserting, retrieving, updating, and removing data from ISC servers. It is possible to add the required Provider, Provider Region, Device and PE Device objects using the APIs.

For details of how to use the ISC APIs, see *Cisco IP Solution Center API Programmer Guide, 4.1* and *Cisco IP Solution Center API Programmer Reference, 4.1*.

2.5.5 Device Configuration Collection

We recommend that a Task Manager Collect Configuration task is used to add interface configuration to Devices in the ISC Repository. A Task Manager Collect Configuration task connects to the physical device in the network, collects the device information from the router (including interface configuration), and populates the ISC Repository with this information.

For details of how to add Device interface configuration using a Task Manager Collect Configuration task, see *Cisco IP Solution Center Infrastructure Reference, 4.1* (**Monitoring > Task Manager**.)

2.5.5.1 Synchronizing the ISC Repository with Device Configuration

Note The accuracy of Cisco MPLS Diagnostics Expert is dependant on up-to-date device information. We recommend that the device configuration is re-synchronized with the physical devices after any configuration changes and at periodic intervals. This ensures that the device configuration held in the ISC inventory is consistent with the physical devices in the network.

We recommend that device configuration is kept up-to-date using a scheduled Task Manager Collect Configuration task. For details of how to create a scheduled Task Manager Collect Configuration task, see *Cisco IP Solution Center Infrastructure Reference, 4.1* (**Monitoring > Task Manager**). All Provider Edge and Provider routers in the MPLS network should have their configuration collected using a scheduled Task Manager Collect Configuration task. The Task Manager Collect Configuration task collects details of interface configuration and other device attributes. The interval at which Task Manager Collect Configuration tasks should be scheduled to run depends on the frequency of configuration changes to the network.

CHAPTER 3

Using Cisco MPLS Diagnostics Expert

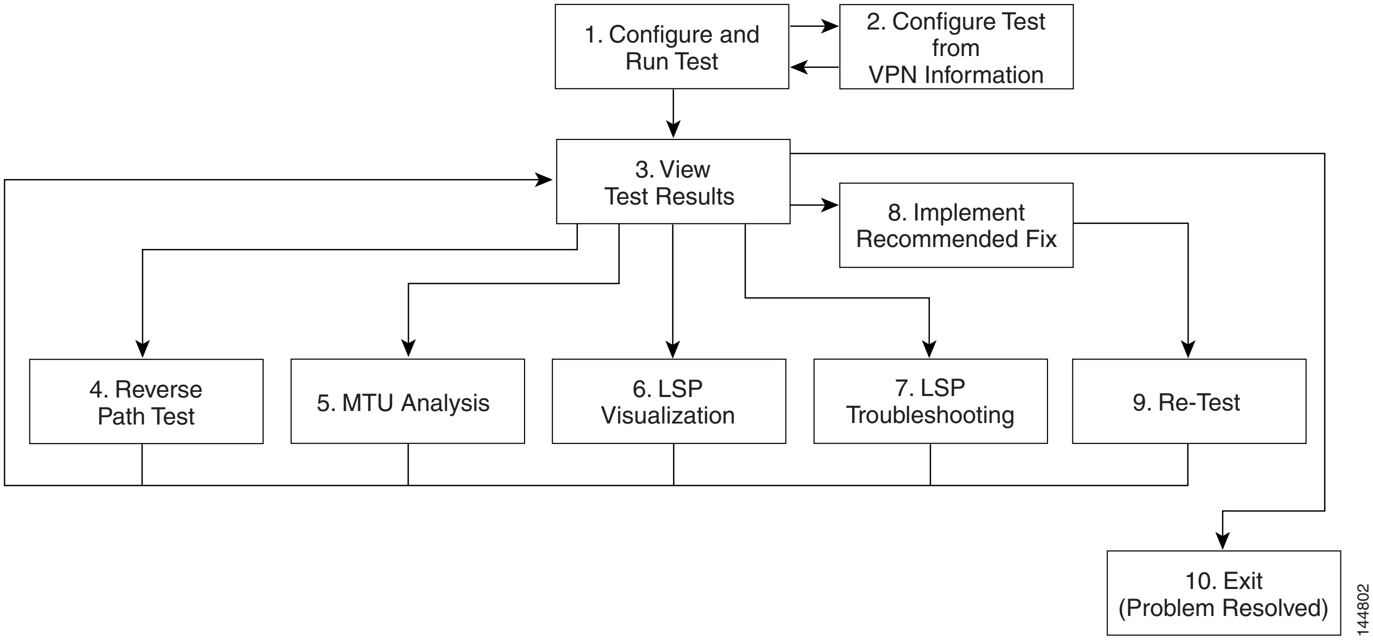
This chapter describes how to use Cisco MPLS Diagnostics Expert.

This chapter contains the following sections:

- 3.1 Performing an MPLS VPN Connectivity Verification Test, page 3-2
- 3.2 Interpreting the Test Results, page 3-16
- 3.3 Advanced Troubleshooting Options, page 3-22

Figure 3-1 describes the workflow for using Cisco MPLS Diagnostics Expert.

Figure 3-1 Using Cisco MPLS Diagnostics Expert Workflow


1. Configure and Run Test
2. Configure Test from VPN Information
3. View Test Results
8. Implement Recommended Fix
4. Reverse Path Test
5. MTU Analysis
6. LSP Visualization
7. LSP Troubleshooting
9. Re-Test
10. Exit (Problem Resolved)
144802

1. Configure and Run Test—Configure and run an MPLS VPN Connectivity Verification test. See 3.1 Performing an MPLS VPN Connectivity Verification Test, page 3-2.
2. Configure Test from VPN Information—Optionally configure an MPLS VPN Connectivity Verification test using VPN information. This is only possible if ISC VPN Provisioning functionality is used to provision VPNs within the network. See 3.1.1 Configuration Using Customer VPN Information, page 3-8.

3. View Test Results—View results of MPLS VPN Connectivity Verification test, including the Test Log. See 3.2 Interpreting the Test Results, page 3-16.
4. Reverse Path Test—Perform Reverse Path Test advanced troubleshooting. See 3.3.1 Reverse Path Testing, page 3-23.
5. MTU Analysis—Perform MTU Analysis advanced troubleshooting. See 3.3.2 MTU Analysis, page 3-23.
6. LSP Visualization—Perform LSP Visualization advanced troubleshooting. See 3.3.3 LSP Visualization, page 3-24.
7. LSP Troubleshooting—Perform LSP Troubleshooting advanced troubleshooting. See 3.3.4 LSP Troubleshooting, page 3-25.
8. Implement Recommended Fix—Manually implement fix as recommended by test results.
9. Re-test—Re-run the MPLS VPN Connectivity Verification test. This would typically be done to verify the fix implemented.

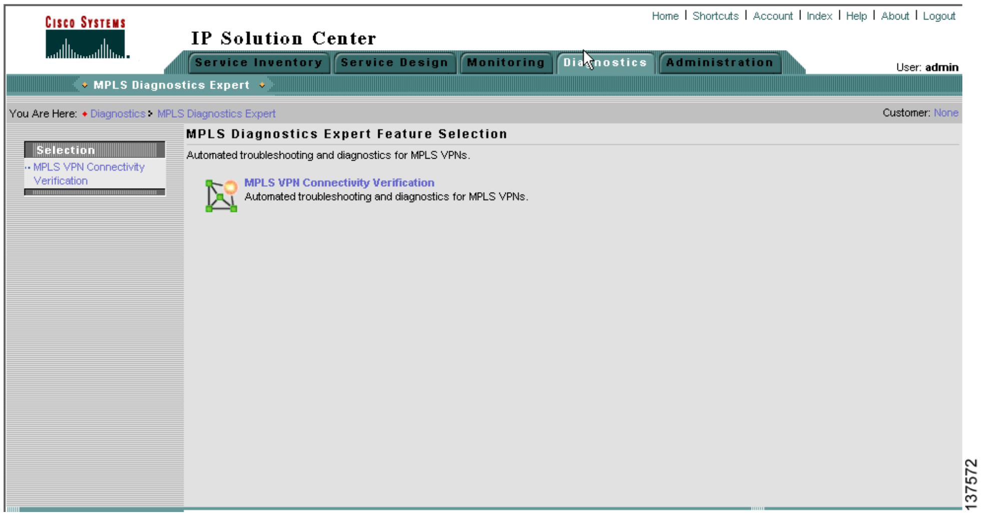
3.1 Performing an MPLS VPN Connectivity Verification Test

This section describes how to perform an MPLS VPN Connectivity Verification test. The Diagnostics tab (see Figure 3-2) allows you to configure this test and to view the results.

Note When performing parallel MPLS VPN Connectivity Verification tests on the same client machine, ensure each test is performed using a different HTTP session. To do so, run each test in a separate browser, launched from the command line, or by clicking on the browser icon on the desktop, or Start menu. Do not run parallel tests in tabs within the same browser window or in browser windows launched from existing browser windows.

Step 1 Click the Diagnostics tab. The MPLS Diagnostics Feature Selection window appears.

Figure 3-2 Diagnostics Tab



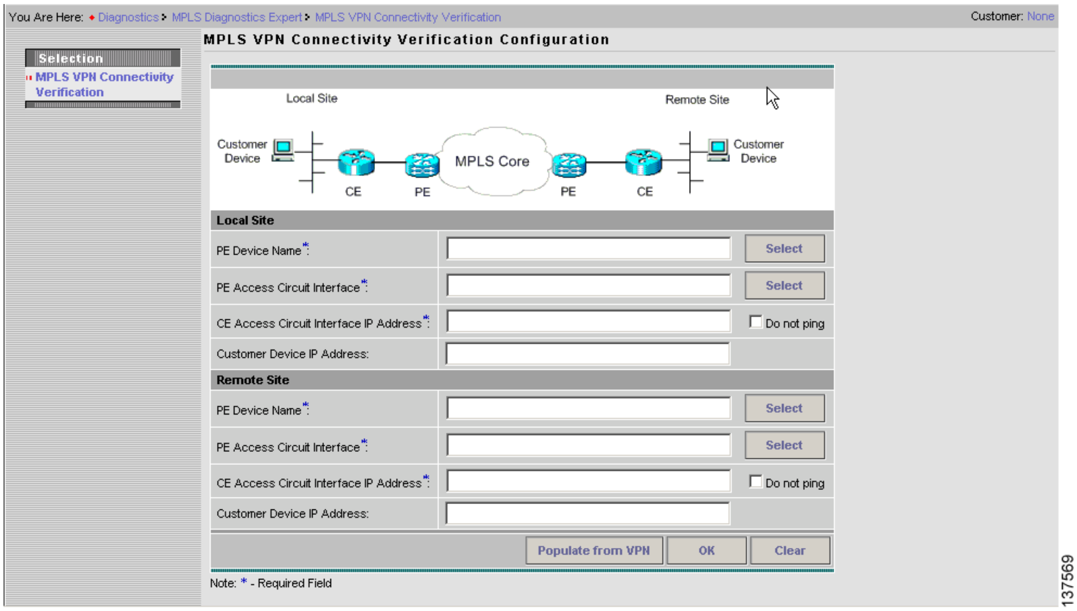
MPLS Diagnostics Expert Feature Selection

Automated troubleshooting and diagnostics for MPLS VPNs.

MPLS VPN Connectivity Verification
Automated troubleshooting and diagnostics for MPLS VPNs.

Step 2 Click on the MPLS VPN Connectivity Verification option. The MPLS VPN Connectivity Verification Configuration window appears (see Figure 3-3).

Figure 3-3 MPLS VPN Connectivity Verification Configuration Window



You Are Here: ♦ Diagnostics > MPLS Diagnostics Expert > MPLS VPN Connectivity Verification — Customer: None

Selection
- MPLS VPN Connectivity Verification

MPLS VPN Connectivity Verification Configuration

Local Site		
PE Device Name*:		Select
PE Access Circuit Interface*:		Select
CE Access Circuit Interface IP Address*:		□ Do not ping
Customer Device IP Address:		
Remote Site		
PE Device Name*:		Select
PE Access Circuit Interface*:		Select
CE Access Circuit Interface IP Address*:		□ Do not ping
Customer Device IP Address:		

Populate from VPN | OK | Clear

Note: * - Required Field

The MPLS VPN Connectivity Verification Configuration window allows you to configure the connectivity test to be performed. This window displays the following components:

- Network diagram
- Local Site configuration area
- Remote Site configuration area

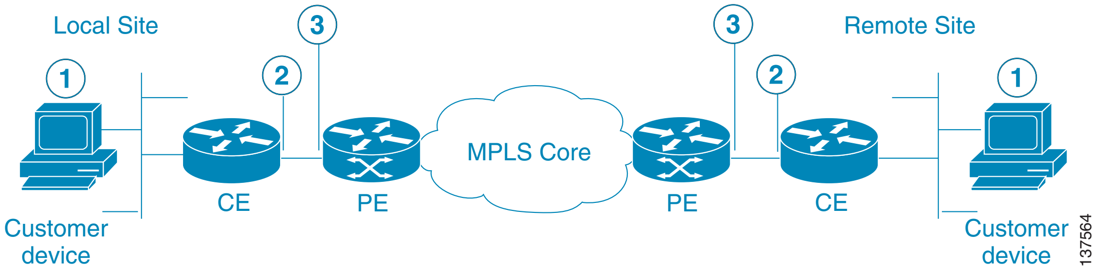
The network diagram is a static image that provides you with context for the information you must enter to configure the test.

MPLS VPN Connectivity Verification tests connectivity between two sites in a VPN. Throughout the test, these sites are referred to as the local site and remote site. It is anticipated that a connectivity problem will be reported or detected from the perspective of a particular site. This particular site would typically be used as the local site, and the test is performed from this site. However, this is not mandatory, as any site can be used as the local or remote site, because connectivity is tested in both directions.

The scope of the L3 VPN connectivity test (see Figure 3-4) can be changed on a per-site basis. For each site you can test connectivity to a customer device within the site (shown on Figure 3-4 as *1*), the CE access circuit interface (shown on Figure 3-4 as *2*), or the PE access circuit interface (shown on Figure 3-4 as *3*). The test scope is determined by the configuration that you provide.

It could be desirable to vary the test scope for a number for reasons. For example, a customer could use an access control list (ACL) on their customer edge (CE) access circuit interface to block ICMP Echo packets from entering the site network. In this instance it would be desirable to limit the test scope to the access circuit interface of the PE device. Alternatively you might want to test to a device within a customer site. A successful test verifies that VPN connectivity exists to that device. If the test to the customer device fails but you are able to verify connectivity between CE devices, this allows you to isolate the problem to the CE device or customer site network.

Figure 3-4 Test Scope



1. Customer device
2. CE access circuit interface
3. PE access circuit interface

By default, if you specify only the required fields for a site, the test is performed to the CE access circuit interface.

Note Required fields are denoted by a blue asterisk in the MPLS VPN Connectivity Verification Configuration window. You will be unable to continue until all required fields have been completed with valid information.

To test connectivity to a device within the customer site subnetwork you should enter the IP address in the Customer Device IP Address field and make sure the **Do not ping** check box is not checked.

To restrict testing to the PE access circuit interface for a site, you should check the **Do not ping** check box located beside the CE Access Circuit Interface IP Address field. If a customer device IP address has been entered, then it is ignored during the test.

Note When testing to the PE access circuit interface, you must enter the CE access circuit interface IP address. This is necessary because automated troubleshooting and diagnostics use the CE IP address to perform configuration checks on the PE device.

Cisco IOS ACLs allow selected traffic to be blocked based on a wide variety of criteria. ACLs configured on the CE can lead to inconsistent results being reported when an MPLS VPN Connectivity Verification test is performed to a customer device or CE interface. Where possible an MPLS VPN Connectivity Verification test will report that traffic is blocked by an ACL configured on the CE device. However, depending on ACL configuration, it is not always possible to determine that traffic is blocked by an ACL configured on the CE device. In some cases an MPLS VPN Connectivity Verification test might report an access circuit failure or unknown failure. In cases where it is suspected that traffic is being blocked at the CE, the test scope should be reduced to the PE access circuit interface.

Step 3 Configure the fields in the MPLS VPN Connectivity Verification Configuration window as required.

Note An alternative way to configure the test is to use customer VPN information. See 3.1.1 Configuration Using Customer VPN Information, page 3-8 for further information.

Table 3-1 provides field descriptions of the MPLS VPN Connectivity Verification Configuration window.

Table 3-1 Field Descriptions for the MPLS VPN Connectivity Verification Configuration Window

Field	Description
Local Site	
PE Device Name (required field)	Enter the local site PE Device Name in the PE Device Name field or select the local site PE Device Name by clicking the Select button. **Note** Clicking the Select button opens the Select PE Device window (see Selecting a PE Device, page 3-6). The Device Name is the fully qualified hostname and domain name of the device. For example, router1.cisco.com. However, the domain name is optional so in many cases the Device Name is the device hostname. For example, router1. The Device Name specified must match that of a PE device with role type of N-PE. For details of how to create PE devices, see 2.5 Inventory Setup, page 2-4.
PE Access Circuit Interface (required field)	Enter the interface name of the local site PE Access Circuit Interface in the PE Access Circuit Interface field or select the local site PE Access Circuit Interface by clicking the Select button. **Note** Clicking the Select button opens the Select Device Interface window (see Selecting a PE Access Circuit Interface, page 3-7). You must specify a valid local PE Device Name before selecting the PE Access Circuit Interface. The interface specified should be the access circuit interface attached to the site's CE. The interface name specified must match an interface on the device, but the interface does not necessarily need to be in the ISC device inventory.
CE Access Circuit Interface IP Address (required field)	Enter the IP address of the CE access circuit interface for the local site. This should be the access circuit interface attached to the specified PE. The IP address entered is validated to ensure it is in the same subnet as the specified PE access circuit interface. The test supports managed and unmanaged Cisco CE devices, and non-Cisco CE devices.
Do not ping (optional field)	Check this check box to restrict connectivity testing to the access circuit interface of the PE device. This option is intended for cases where the customer has blocked access to the CE interface, for example, when using an ACL.
Customer Device IP Address (optional field)	Enter the IP address of a customer device on the local site customer network. Entering the customer device IP address causes the connectivity test to be performed to this device.
Remote Site	
PE Device Name (required field)	Enter the remote site PE Device Name in the PE Device Name field or select the remote site PE Device Name by clicking the Select button. **Note** Click the Select button to open the Select PE Device window (see Selecting a PE Device, page 3-6). The Device Name is the fully qualified hostname and domain name of the device. For example, router1.cisco.com. However, the domain name is optional so in many cases the Device Name is the device hostname. For example, router1. The Device Name specified must match that of a PE device with role type of N-PE. For details of how to create PE devices, see 2.5 Inventory Setup, page 2-4.

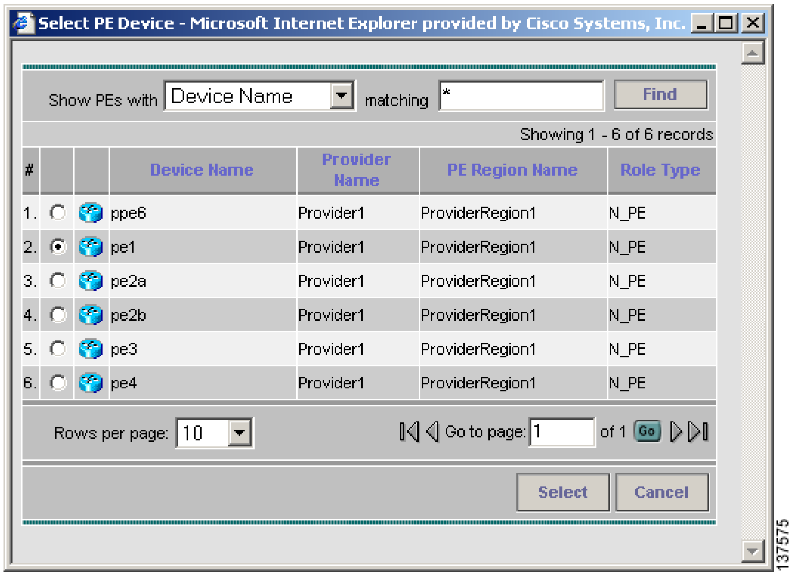
Table 3-1 Field Descriptions for the MPLS VPN Connectivity Verification Configuration Window (continued)

Field	Description
PE Access Circuit Interface (required field)	Enter the interface name of the remote site PE Access Circuit Interface in the PE Access Circuit Interface field or select the remote site PE Access Circuit Interface by clicking the Select button. Click the Select button to open the Select Device Interface window (see Selecting a PE Access Circuit Interface, page 3-7). You must specify a valid remote PE Device Name before selecting the PE Access Circuit Interface. The interface specified should be the access circuit interface attached to the site's CE. The interface name specified must match an interface on the device, but the interface does not necessarily need to be in the ISC device inventory.
CE Access Circuit Interface IP Address (required field)	Enter the IP address of the CE access circuit interface for the remote site. This should be the access circuit interface attached to the specified PE. The IP address entered is validated to ensure it is in the same subnet as the specified PE access circuit interface. The test supports managed and unmanaged Cisco CE devices, and non-Cisco CE devices.
Do not ping (optional field)	Check this check box to restrict connectivity testing to the access circuit interface of the PE device. This option is intended for cases where the customer has blocked access to the CE interface, for example, when using an access list.
Customer Device IP Address (optional field)	Enter the IP address of a customer device on the remote site customer network. Entering the customer device IP address causes the connectivity test to be performed to this device.
Buttons	
Populate from VPN	Click the Populate from VPN button to open the Populate from VPN window. The Populate from VPN window allows you to configure the test using customer VPN information (see 3.1.1 Configuration Using Customer VPN Information, page 3-8.)
OK	Click **OK** to run the test.
Clear	Click **Clear** to reset all the fields in the window.

Selecting a PE Device

Click the Select button (for the Local/Remote PE Device Name) to open the Select PE Device window (see Figure 3-5) where you can choose the local/remote site PE. The Select PE Device window displays a table containing all the PE devices available in the inventory.

Figure 3-5 Select PE Device Window


Select PE Device - Microsoft Internet Explorer provided by Cisco Systems, Inc.
Find
Select
Cancel
Go
137575

Show PEs with Device Name matching *

Showing 1 - 6 of 6 records

#			Device Name	Provider Name	PE Region Name	Role Type
1.	○		ppe6	Provider1	ProviderRegion1	N_PE
2.	●		pe1	Provider1	ProviderRegion1	N_PE
3.	○		pe2a	Provider1	ProviderRegion1	N_PE
4.	○		pe2b	Provider1	ProviderRegion1	N_PE
5.	○		pe3	Provider1	ProviderRegion1	N_PE
6.	○		pe4	Provider1	ProviderRegion1	N_PE

Rows per page: 10

Go to page: 1 of 1

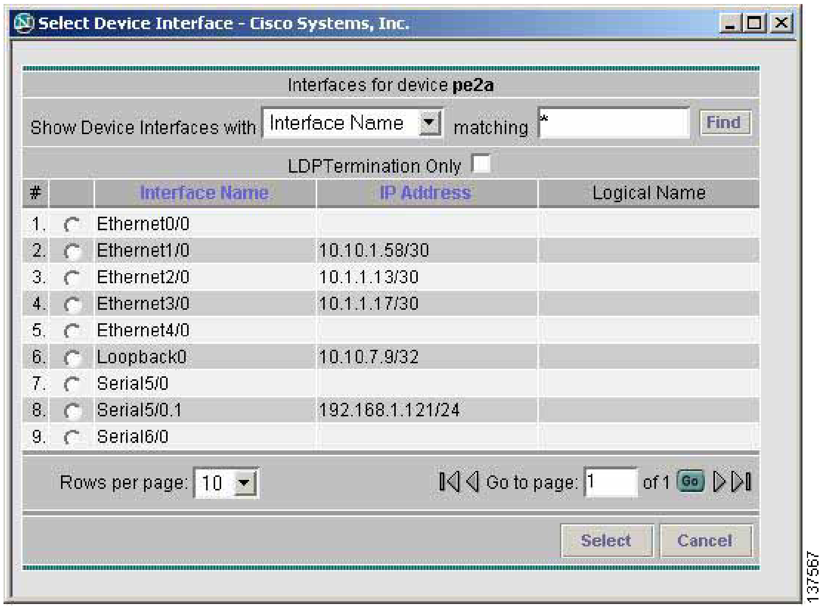
You can perform a wildcard string search of all PE attributes displayed in the PE table. If you select a local/remote site PE from the ISC inventory, this overrides anything entered in the Local/Remote PE Device Name field (see Figure 3-3.)

Selecting a PE Access Circuit Interface

Click the Select button (for the Local/Remote PE Access Circuit Interface) to open the Select Device Interface window (see Figure 3-6) where you can choose the interface name. The Select Device Interface window displays a table containing all interfaces for the selected local/remote PE device.

Note The LDP Termination Only check box is used to filter for LDP terminating loopback interfaces in cases where selection of an LDP terminating loopback interface is required. This check box should be left unchecked.

Figure 3-6 Select Device Interface Window



Interfaces for device **pe2a**

Show Device Interfaces with: Interface Name ▾ matching: * [Find]

LDPTermination Only □

#		Interface Name	IP Address	Logical Name
1.	○	Ethernet0/0		
2.	○	Ethernet1/0	10.10.1.58/30	
3.	○	Ethernet2/0	10.1.1.13/30	
4.	○	Ethernet3/0	10.1.1.17/30	
5.	○	Ethernet4/0		
6.	○	Loopback0	10.10.7.9/32	
7.	○	Serial5/0		
8.	○	Serial5/0.1	192.168.1.121/24	
9.	○	Serial6/0		

Rows per page: 10 ▾ Go to page: 1 of 1 [Go]

[Select] [Cancel]

You can perform a wildcard string search of all attributes displayed in the table. If you select a Local/Remote PE Access Circuit Interface from the ISC inventory, this overrides anything entered in the Local/Remote PE Access Circuit Interface field (see Figure 3-3).

Step 4 Click **OK** to run the test after all the required fields are completed. The Progress window appears (see Figure 3-10 on page 3-15).

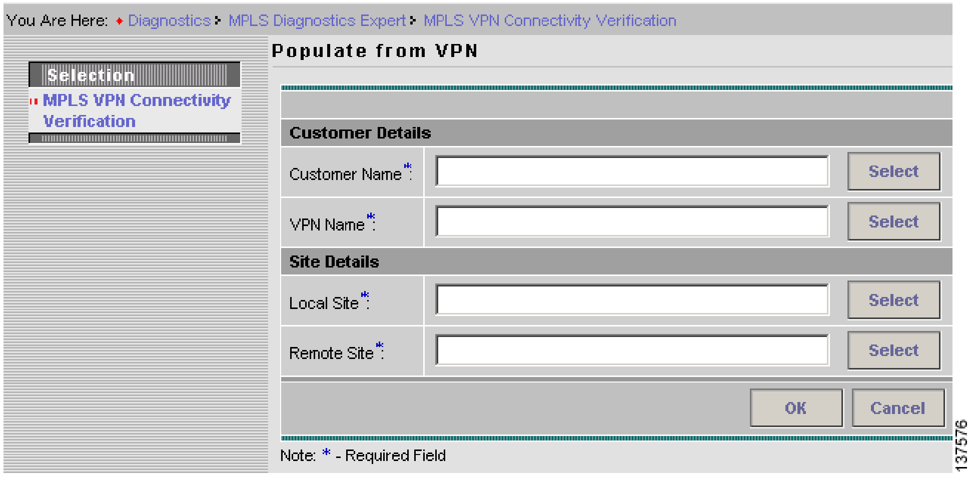
3.1.1 Configuration Using Customer VPN Information

Cisco MPLS Diagnostics Expert can be used standalone, without any dependency on other ISC functionality. However, if ISC VPN Provisioning functionality is used to provision VPNs within the network, this provisioning information, associated with the customer and VPN, can be used as an alternative means to configure an MPLS VPN Connectivity Verification test. Rather than specifying device-specific configuration, you can specify a customer, VPN, local site, and remote site. All required test configuration is then derived from this information.

Note The option to configure an MPLS VPN Connectivity Verification test using customer VPN information is only available if the ISC VPN Provisioning functionality is used to provision VPNs within the network.

Step 1 Click the Populate from VPN button in the MPLS VPN Connectivity Verification window. The Populate from VPN window appears (see Figure 3-7).

Figure 3-7 Populate from VPN Window



Step 2 Configure the fields displayed in the Populate from VPN window. Table 3-2 provides field descriptions for the Populate from VPN window.

Table 3-2 Field Descriptions for the Populate from VPN Window

Field	Description
Customer Name (required field)	Click the Select button to select a customer from the Select Customer pop-up window.
VPN Name (required field)	Click the Select button to select a VPN name from the VPN Name pop-up window. **Note** You must select a Customer Name before you can select a VPN Name.
Local Site (required field)	Click the Select button to select a Local Site from the Local Site pop-up window. **Note** You must select a Customer Name and a VPN Name before you can select a local site.
Remote Site (required field)	Click the Select button to select a Remote Site from the Remote Site pop-up window. **Note** You must select a Customer Name and VPN Name before you can select a remote site.

Step 3 Click **OK**. The MPLS VPN Connectivity Verification Configuration window reappears. The required fields are populated based on the customer VPN information you provided in the Populate from VPN window.

Note If you want to test to a customer device you can enter the IP address in the Local and/or Remote Site Customer Device IP Addresses fields.

Note You can edit any of the fields in the MPLS VPN Connectivity Verification Configuration window that have been automatically populated.

Step 4 Click **OK** on the MPLS VPN Connectivity Verification Configuration window to run the test. The Progress window appears (see Figure 3-10 on page 3-15).

3.1.2 VPN Topologies

By default an MPLS VPN Connectivity Verification test assumes that the local and remote sites are connected through a full mesh VPN topology and that these sites can communicate directly. If the sites being tested are connected through a VPN topology other than full mesh, the required configuration for an MPLS VPN Connectivity Verification test might differ. In this situation the test might produce misleading results, so you must take care when interpreting the test results. The following sections detail the configuration required and how the test results should be interpreted for each supported VPN topology.

3.1.2.1 Testing with Hub and Spoke VPN Topology

Customer sites connected through a hub and spoke VPN cannot communicate directly. The customer sites (Spokes) communicate through a Hub router. When testing connectivity between two sites connected through a hub and spoke VPN you should perform the test using the following steps:

Step 1 MPLS VPN Connectivity Verification test between the local and the remote sites.

Step 2 MPLS VPN Connectivity Verification test between the local site and the hub CE interface that is attached to the hub PE interface importing routes.

Step 3 MPLS VPN Connectivity Verification test between the remote site and the hub CE interface that is attached to the hub PE interface importing routes.

Step 4 MPLS VPN Connectivity Verification test between the local site and the hub CE interface that is attached to the hub PE interface exporting routes.

Step 5 MPLS VPN Connectivity Verification test between the remote site and the hub CE interface that is attached to the hub PE interface exporting routes.

Note After fixing a problem reported in Step 1 though Step 5, you should repeat Step 1 to verify that connectivity between the sites has been restored.

Note If a connectivity failure is detected in Step 1 due to an access circuit or VPN edge problem, then the problem will be correctly diagnosed by the MPLS VPN Connectivity Verification test performed in Step 1. You should rectify the problem as described by the text results. If the connectivity failure is due to a problem within the core of the hub and spoke MPLS VPN, then the result reported by Step 1 will be incorrect and should be ignored. Step 2 though Step 5 should be performed until the problem is diagnosed correctly.

Each step involves performing an MPLS VPN Connectivity Verification test between different points. Depending on whether a connectivity failure exists and the location of this failure, it might not be necessary to perform all five steps. Figure 3-7 shows the workflow for testing a hub and spoke VPN.

Figure 3-8 Workflow

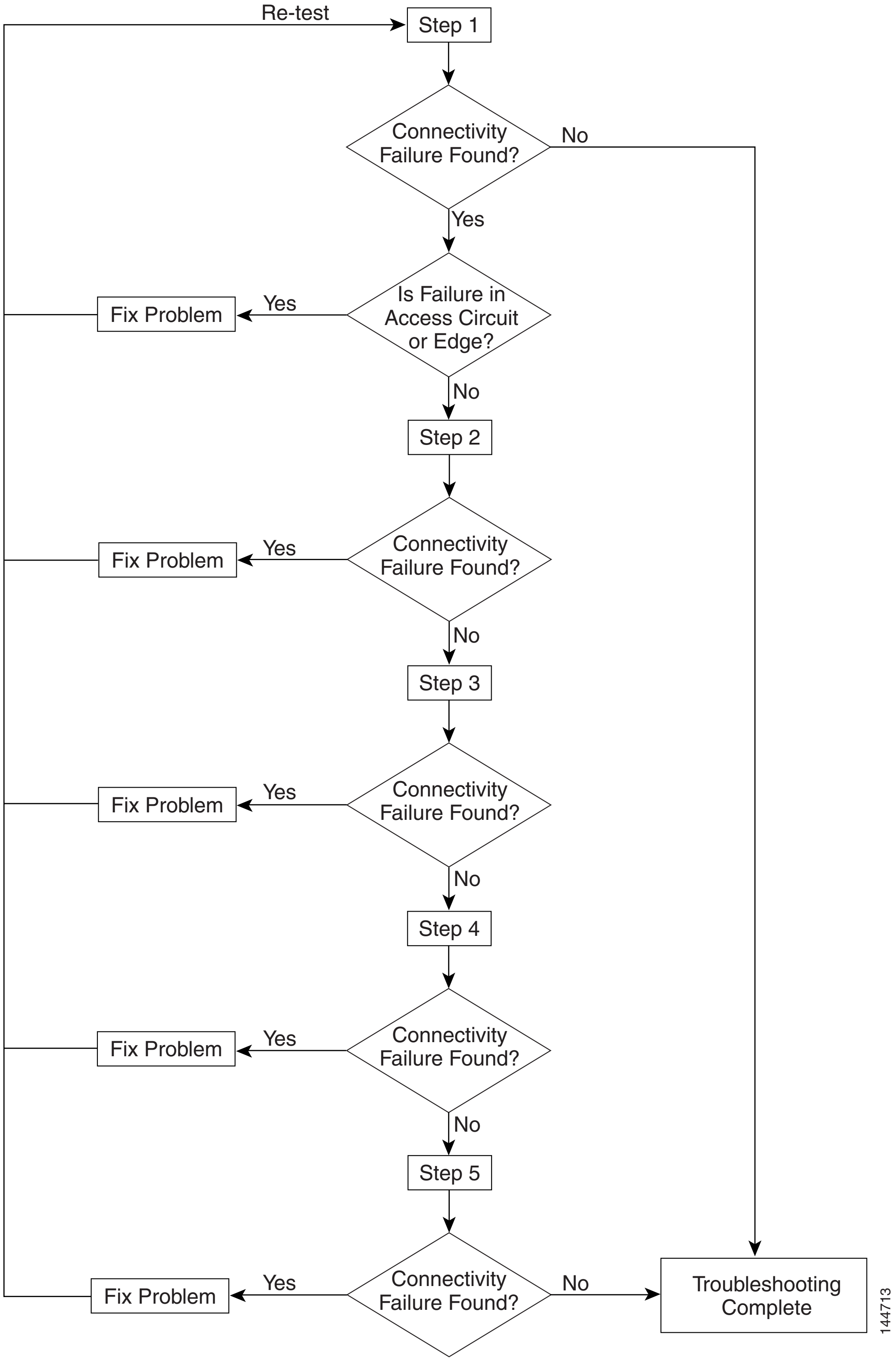
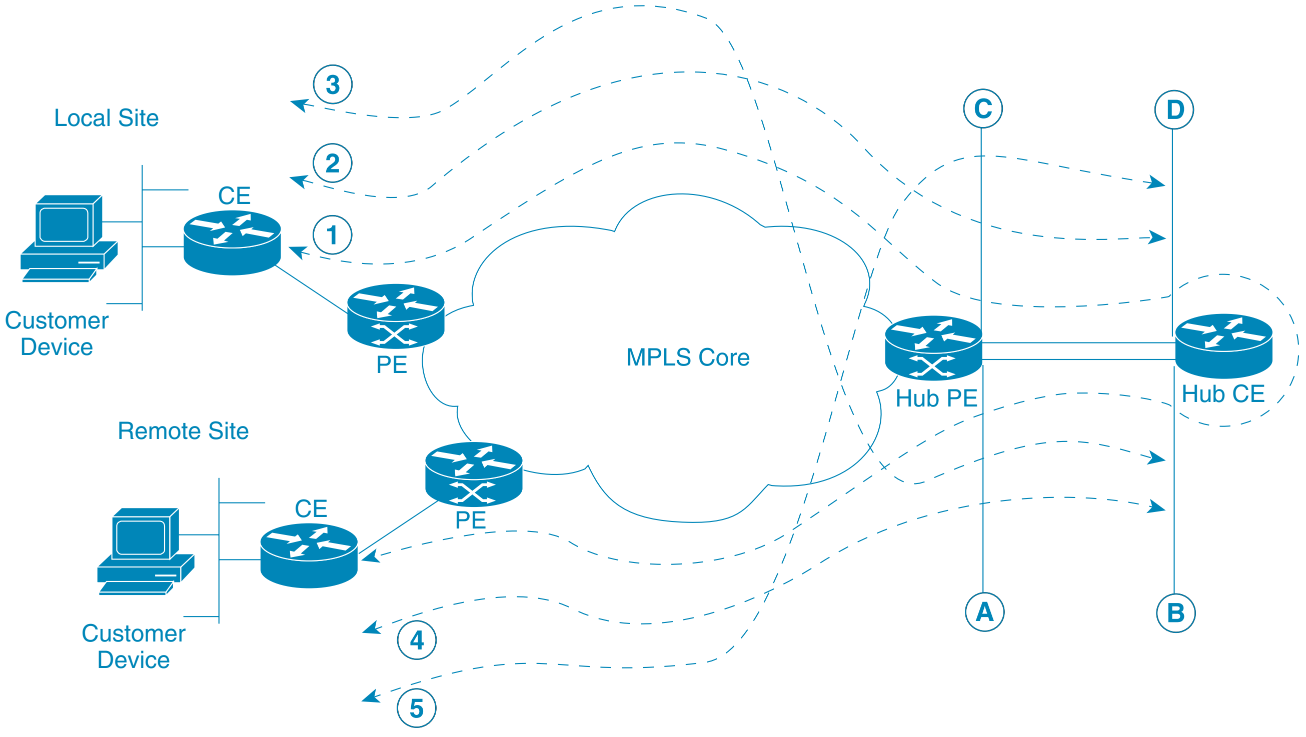

Re-test
Step 1
Connectivity Failure Found?
No
Yes
Is Failure in Access Circuit or Edge?
Yes
Fix Problem
No
Step 2
Connectivity Failure Found?
Yes
Fix Problem
No
Step 3
Connectivity Failure Found?
Yes
Fix Problem
No
Step 4
Connectivity Failure Found?
Yes
Fix Problem
No
Step 5
Connectivity Failure Found?
Yes
Fix Problem
No
Troubleshooting Complete
144713

Figure 3-9 illustrates the MPLS VPN Connectivity Verification tests required to test connectivity between two sites in a hub and spoke VPN.

Figure 3-9 Testing a Hub and Spoke VPN Topology



A Hub PE interface importing routes.

B Hub CE interface directly connected to hub PE interface importing routes.

C Hub PE interface exporting routes.

D Hub CE interface directly connected to hub PE interace exporting routes.

1 to 5 illustrates tests performed in steps 1 through 5.

Step 1 Involves performing an MPLS VPN Connectivity Verification test between the local and remote sites. If this test finds no connectivity problems, then no further troubleshooting is required. If this test reports a connectivity failure caused by an MPLS problem, you should ignore the test result and move to Step 2. As an MPLS VPN Connectivity Verification test assumes a full mesh VPN topology, the problem reported will be incorrect. You must perform further MPLS VPN Connectivity Verification tests to identify the problem on a hub and spoke VPN. If this test reports a connectivity failure caused by a non-MPLS problem (for example, access circuit or VPN edge failure), then you should fix the problem as reported and retest.

Note If a connectivity failure is found, the MPLS VPN Connectivity Verification test performed in Step 1 will detect that a hub and spoke VPN topology is being tested and advise you to perform hub and spoke specific troubleshooting as described in the following steps. The MPLS VPN Connectivity Verification test detects a hub and spoke VPN topology by checking the Route Target imports and exports. If the same Route Target is imported and exported by one or both PE routers, then a hub and spoke VPN is assumed.

Step 2 Involves performing an MPLS VPN Connectivity Verification test between the local site (Spoke) and the hub CE interface that is attached to the hub PE interface which imports routes (shown on Figure 3-9 as *A*). When configuring the MPLS VPN Connectivity Verification test, the Local Site fields on the MPLS VPN Connectivity Verification Configuration window should be configured with details of the local customer site. The Remote Site fields should be configured with details of the Hub PE/CE interface which imports routes (shown on Figure 3-9 as *A*), as shown in Table 3-3.

Step 3 Involves performing an MPLS VPN Connectivity Verification test between the remote site (Spoke) and the hub CE interface that is attached to the hub PE interface which imports routes (shown on Figure 3-9 as *A*). When configuring the MPLS VPN Connectivity Verification test, the Local Site fields should be configured with details of the Hub PE interface which imports routes (shown on Figure 3-9 as *A*), as shown in Table 3-3. The Remote Site fields on the MPLS VPN Connectivity Verification Configuration window should be configured with details of the remote customer site.

Table 3-3 MPLS VPN Connectivity Verification Test Configuration—Hub PE Route Import Interface Test

Field Name	Hub Detail
PE Device Name	Hub PE Device Name.
PE Access Circuit Interface	Hub PE Interface which imports routes.
CE Access Circuit Interface IP Address	IP Address of Hub CE Interface directly connected to PE interface which imports routes.
Customer Device IP Address	Leave blank.

Step 4 Involves performing an MPLS VPN Connectivity Verification test between the local site (Spoke) and the hub CE interface that is attached to the hub PE interface which exports routes (shown on Figure 3-9 as *C*). When configuring the MPLS VPN Connectivity Verification test, the Local Site fields on the MPLS VPN Connectivity Verification Configuration window should be configured with details of the local customer site. The Remote Site fields should be configured with details of the Hub PE interface which exports routes (shown on Figure 3-9 as *C*), as shown in Table 3-4.

Step 5 Involves performing an MPLS VPN Connectivity Verification test between the remote site (Spoke) and the hub CE interface that is attached to the hub PE interface which exports routes (shown on Figure 3-9 as *C*). When configuring the MPLS VPN Connectivity Verification test, the Local Site fields should be configured with details of the Hub PE interface which exports routes (shown on Figure 3-9 as *C*), as shown in Table 3-4. The Remote Site fields on the MPLS VPN Connectivity Verification Configuration window should be configured with details of the remote customer site.

Table 3-4 MPLS VPN Connectivity Verification Test Configuration —Hub PE Route Export Interface Test

Field Name	Hub Detail
PE Device Name	Hub PE Device Name.
PE Access Circuit Interface	Hub PE Interface which exports routes.
CE Access Circuit Interface IP Address	IP Address of Hub CE Interface directly connected to PE interface which exports routes.
Customer Device IP Address	Leave blank.

3.1.2.2 Testing with Intranet/Extranet VPN Topology

Sites connected through an Intranet/Extranet VPN topology can communicate directly, similar to a full mesh VPN topology. When configuring an MPLS VPN Connectivity Verification test between two sites connected through an Intranet/Extranet VPN you should configure the test as normal.

When testing connectivity between sites connected through an Intranet/Extranet VPN, Cisco MPLS Diagnostics Expert will troubleshoot MPLS VPN connectivity issues including access circuit, VPN edge and MPLS core problems. Cisco MPLS Diagnostics Expert does not troubleshoot Intranet/Extranet VPN specific problems, such as missing or miss-configured route maps.

If an MPLS VPN Connectivity Verification test detects a connectivity failure but that failure cannot be attributed to MPLS VPN connectivity issues including access circuit, VPN edge and MPLS core problems, then the Test Results window will recommend that you troubleshoot the Intranet/Extranet configuration.

Note Cisco MPLS Diagnostics Expert assumes a possible Intranet/Extranet VPN topology if it finds Route Maps configured on either PE.

3.1.2.3 Testing with Central Services VPN Topology

With a Central Services VPN topology the client sites can communicate directly with one or more central sites, but they cannot communicate with each other. When configuring an MPLS VPN Connectivity Verification test between a client site and central site, connected through a Central Services VPN topology, you should configure the test as normal by entering the client site and central site, as the local and remote site respectively.

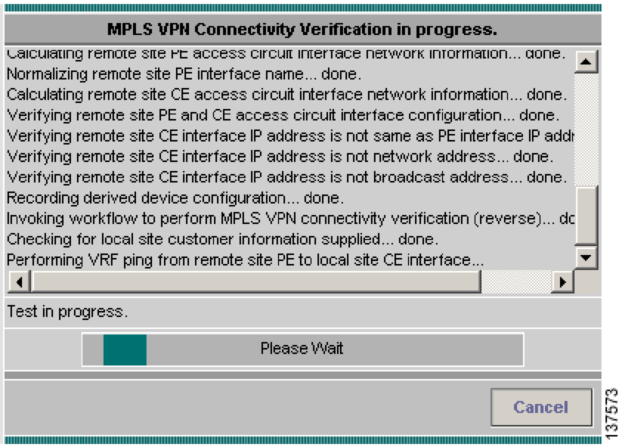
It is not possible to perform an MPLS VPN Connectivity Verification test between two client sites in a Central Services VPN.

3.1.3 Progress Window

The time taken to perform an MPLS VPN Connectivity Verification test varies. A test could take some time to complete, depending on the size of your network, whether a connectivity problem is identified, and the nature of this connectivity problem. While the test is being performed the Progress window is displayed (see Figure 3-10).

The Progress window displays a one-line textual summary of each step that has been completed and the step that is currently executing.

Figure 3-10 *Progress Window*



MPLS VPN Connectivity Verification in progress.

```
Calculating remote site PE access circuit interface network information... done.
Normalizing remote site PE interface name... done.
Calculating remote site CE access circuit interface network information... done.
Verifying remote site PE and CE access circuit interface configuration... done.
Verifying remote site CE interface IP address is not same as PE interface IP addr
Verifying remote site CE interface IP address is not network address... done.
Verifying remote site CE interface IP address is not broadcast address... done.
Recording derived device configuration... done.
Invoking workflow to perform MPLS VPN connectivity verification (reverse)... dc
Checking for local site customer information supplied... done.
Performing VRF ping from remote site PE to local site CE interface...
```

Test in progress.

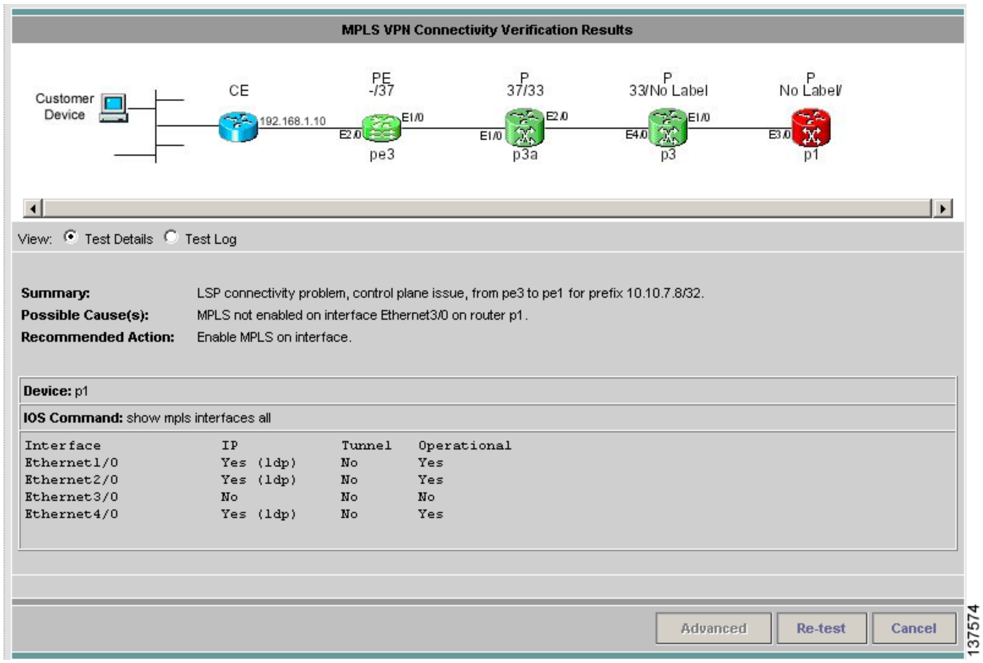
Click the Cancel button to cancel the test if required. If you click **Cancel**, you are asked to confirm that you want to cancel the test. If you confirm, the test is cancelled when the current step has completed. If the current step involves device interaction, this completes before the test is cancelled. Upon cancellation, the Test Results window appears indicating that you cancelled the test. All completed steps are displayed in the test log.

When the test is complete the Test Results window appears. See 3.2 Interpreting the Test Results, page 3-16, for further details.

3.2 Interpreting the Test Results

Upon completion of a MPLS VPN Connectivity Verification test, the Test Results window appears (see Figure 3-11).

Figure 3-11 Test Results Window with Failure Specific Additional Information Displayed



MPLS VPN Connectivity Verification Results

View: ● Test Details ○ Test Log

Summary: LSP connectivity problem, control plane issue, from pe3 to pe1 for prefix 10.10.7.8/32.

Possible Cause(s): MPLS not enabled on interface Ethernet3/0 on router p1.

Recommended Action: Enable MPLS on interface.

Device: p1

IOS Command: show mpls interfaces all

```
Interface              IP            Tunnel   Operational
Ethernet1/0            Yes (ldp)     No       Yes
Ethernet2/0            Yes (ldp)     No       Yes
Ethernet3/0            No            No       No
Ethernet4/0            Yes (ldp)     No       Yes
```

Advanced | Re-test | Cancel

The Test Result window displays the location and cause of the problem found, recommended actions, observations, and details of the automated troubleshooting and diagnostics steps performed. The Test Result window also allows you to invoke advanced troubleshooting options where appropriate (see Table 3-5).

The Test Results window consists of the following components:

Table 3-5 Field Descriptions for the Test Results Window

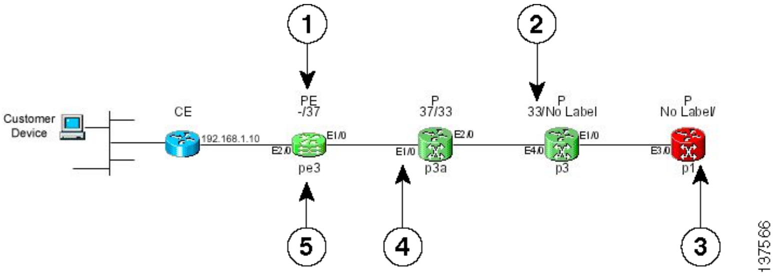
Field/Button	Description
Data path	See 3.2.1 Data Path, page 3-17
Test Details	See 3.2.2 Test Details, page 3-19
Test Log	See 3.2.3 Test Log, page 3-21
Export button	The Export button appears when the Test Log radio button is selected. See 3.2.4 Export, page 3-22.
Advanced button	Click the Advanced button to launch advanced troubleshooting. See 3.3 Advanced Troubleshooting Options, page 3-22. The options available on this button are dynamically configured depending on the test result. In some cases there might be no advanced troubleshooting options available.
Re-test button	Click the Re-test button to re-run the connectivity test using the existing configuration. This can be used to verify the fix implemented.
Cancel button	Click the Cancel button to cancel the current test and return to the Test Configuration window. You will not be asked to confirm cancellation.

Note The Test Result window displays details of the first failure found. If multiple failures exist, subsequent failures are not reported until the current failure is fixed and the test is re-run.

3.2.1 Data Path

The Data Path (see Figure 3-12) shows a graphical representation of the path between the two sites that have been tested.

Figure 3-12 Data Path



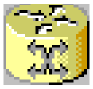
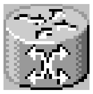
1. Device Role (CE, PE, or P).
2. MPLS labels (ingress/egress).
3. Failed device.
4. IOS interface name.
5. Device hostname.

If a failure is found, the data path highlights the failed device or link. The device colors used in the data path are described in Table 3-6.

Table 3-6 Data Path Device Color Codes

Color	Icon	Description
Green	🟩	Device has been tested and is functioning normally.
Blue	🟦	Device has not been tested or status is unknown.
Red	🟥	Device failure.

Table 3-6 Data Path Device Color Codes (continued)

Color	Icon	Description
Yellow		Possible device failure.
Grey		Device access failure.

The link color used in the data path is described in Table 3-7.

Table 3-7 Data Path Link Color Code

Color	Icon	Description
Red		A connectivity failure has been found. This failure might be due to a problem on one or both attached devices.

For each core PE and P device, the following information is displayed:

- Role (PE or P)
- Device name
- Interface names
- Ingress and egress MPLS labels (MPLS core failures only)

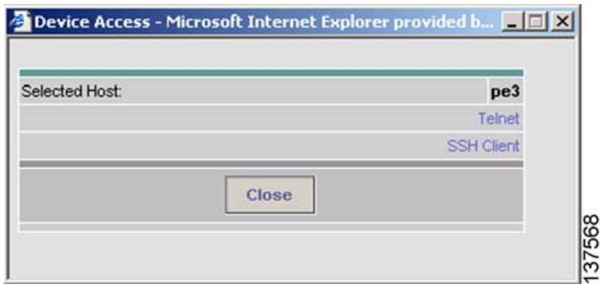
The information displayed for CE devices and customer devices is minimal. Typically only the information provided during test configuration is displayed for these devices.

3.2.1.1 Device Actions

PE and P devices displayed in the Data Path support the invocation of device-specific actions. Device specific actions are invoked by left-clicking on the appropriate device within the data path. You can then select the action to invoke from a pop-up dialog (see Figure 3-13). The currently supported device actions are Telnet and SSH.

Note When connecting to a device through Telnet or SSH, you must enter the appropriate device authentication, as configured on that device.

Figure 3-13 Device Actions



Selected Host: pe3

The ability to launch device actions can be disabled using user roles. See 2.3 User Roles, page 2-3 for further details.

Note Invoking a Telnet or SSH device action will attempt to run the default Telnet or SSH application configured on the client machine. If no application is configured, then the browser-specific error handling occurs.

Note Telnet and SSH device actions are launched from the client machine from which the browser is running. If this machine does not have a route to the managed device, the action will fail.

3.2.2 Test Details

The Test Details section of the Test Results window (see Figure 3-11 on page 3-16) displays a summary of the automated troubleshooting and diagnostics results, observations made during troubleshooting, additional failure-specific information, and recommended action.

The Test Details summary is displayed in all cases. The test details summary consists of three fields that detail:

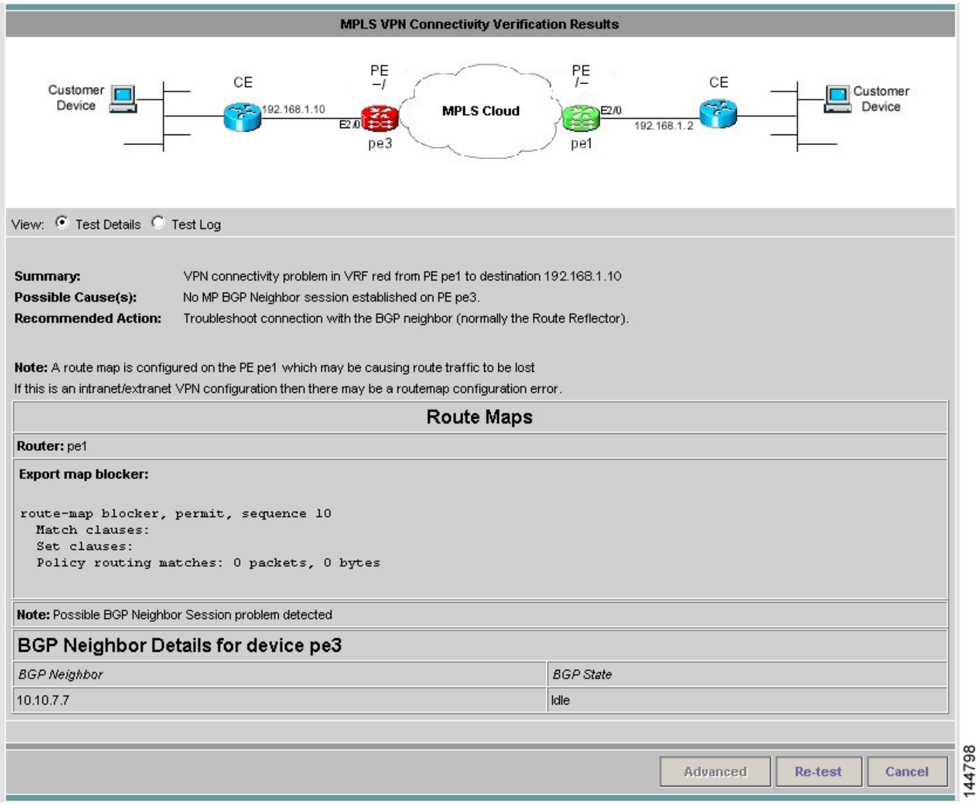
- Summary—Displays a brief summary of the failure found.
- Possible Cause(s)—Possible causes of the failure.
- Recommended Action—Recommended actions to resolve the problem.

Failure-specific additional information is displayed below the summary as required. When displayed, this provides additional information on the problem found. For example, Forwarding Information Base (FIB), Label Forwarding Information Base (LFIB), BGP table entries, and route target import/exports. This additional failure specific information helps highlight problems such as FIB, LFIB, BGP inconsistencies, and route target import/export mismatches. For some failures no additional information is displayed.

Figure 3-11 on page 3-16 shows an example Test Results window with failure specific information below the Test Details summary.

The Test Details radio button is selected by default.

Figure 3-14 Test Results Window with Observation Notes



View: ● Test Details ○ Test Log

Summary: VPN connectivity problem in VRF red from PE pe1 to destination 192.168.1.10
Possible Cause(s): No MP BGP Neighbor session established on PE pe3.
Recommended Action: Troubleshoot connection with the BGP neighbor (normally the Route Reflector).

Note: A route map is configured on the PE pe1 which may be causing route traffic to be lost
If this is an intranet/extranet VPN configuration then there may be a routemap configuration error.

Route Maps

Router: pe1

Export map blocker:

```
route-map blocker, permit, sequence 10
  Match clauses:
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
```

Note: Possible BGP Neighbor Session problem detected

BGP Neighbor Details for device pe3

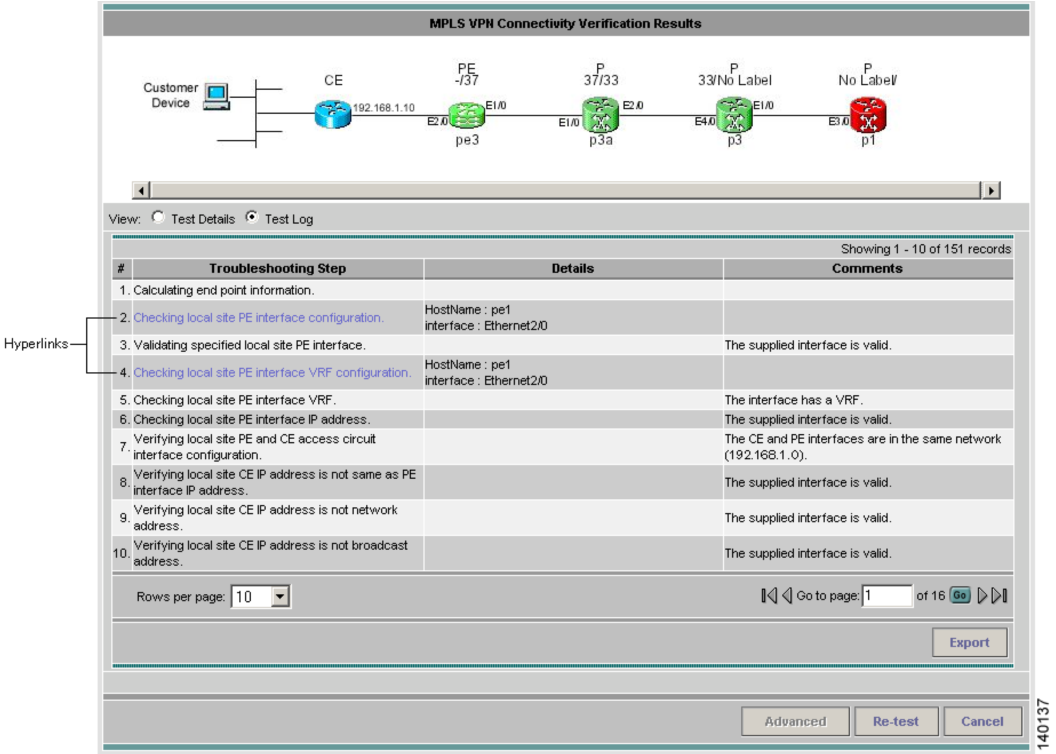
BGP Neighbor	*BGP State*
10.10.7.7	Idle

Observations made during troubleshooting are displayed as notes below the Test Details summary. Observation notes detail observations made during troubleshooting which could be related to the failure. They should be considered as additional troubleshooting information. Figure 3-14 shows an example Test Results window with two observation notes. In some cases no observation notes are displayed, while in other cases multiple notes might be displayed.

3.2.3 Test Log

Click the Test Log (see Figure 3-15) radio button to display details of all troubleshooting and diagnostics steps in the order in which they were performed.

Figure 3-15 Test Results Window—Test Log



MPLS VPN Connectivity Verification Results

View: ○ Test Details ● Test Log

Showing 1 - 10 of 151 records

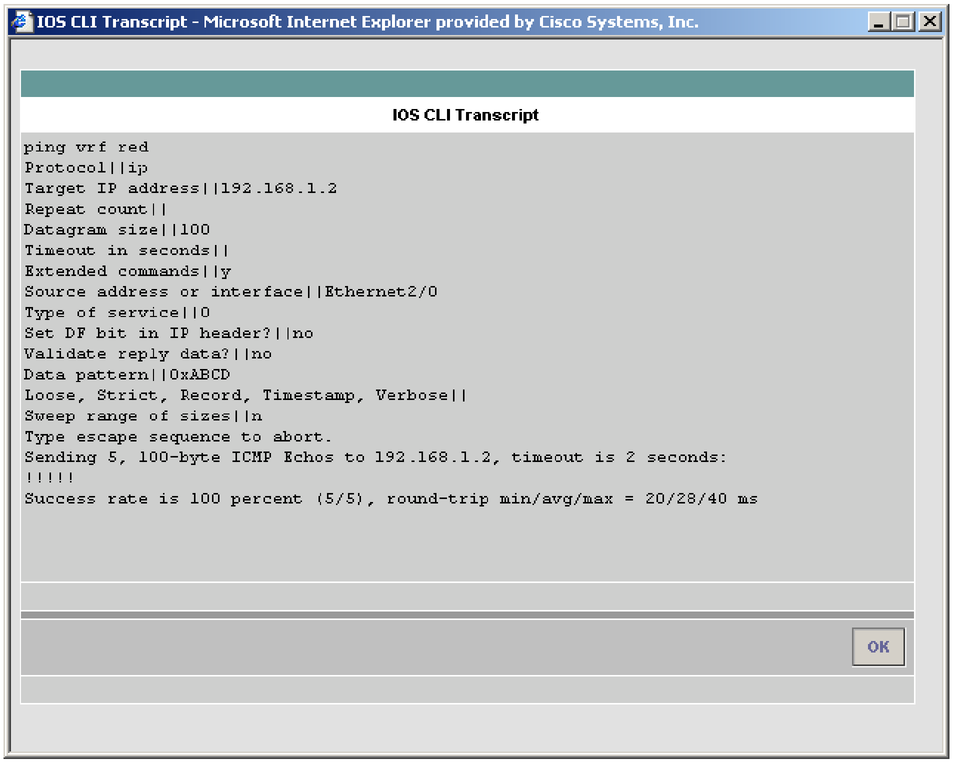
#	Troubleshooting Step	Details	Comments
1.	Calculating end point information.		
2.	Checking local site PE interface configuration.	HostName : pe1 interface : Ethernet2/0	
3.	Validating specified local site PE interface.		The supplied interface is valid.
4.	Checking local site PE interface VRF configuration.	HostName : pe1 interface : Ethernet2/0	
5.	Checking local site PE interface VRF.		The interface has a VRF.
6.	Checking local site PE interface IP address.		The supplied interface is valid.
7.	Verifying local site PE and CE access circuit interface configuration.		The CE and PE interfaces are in the same network (192.168.1.0).
8.	Verifying local site CE IP address is not same as PE interface IP address.		The supplied interface is valid.
9.	Verifying local site CE IP address is not network address.		The supplied interface is valid.
10.	Verifying local site CE IP address is not broadcast address.		The supplied interface is valid.

Rows per page: 10

Go to page: 1 of 16 Go

Some steps require device interaction involving the execution of IOS CLI commands. These steps appear in the Test Log as hyperlinks. Clicking a hyperlink opens a pop-up window that displays the IOS CLI transcript for the step (see Figure 3-16). This transcript includes the IOS commands run and all resulting output.

Figure 3-16 IOS CLI Transcript Window


IOS CLI Transcript - Microsoft Internet Explorer provided by Cisco Systems, Inc.
IOS CLI Transcript
OK
140198

```
ping vrf red
Protocol||ip
Target IP address||192.168.1.2
Repeat count||
Datagram size||100
Timeout in seconds||
Extended commands||y
Source address or interface||Ethernet2/0
Type of service||0
Set DF bit in IP header?||no
Validate reply data?||no
Data pattern||0xABCD
Loose, Strict, Record, Timestamp, Verbose||
Sweep range of sizes||n
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/28/40 ms
```

3.2.4 Export

You might want to export the test log to include it in a trouble ticket, problem escalation, or when contacting Cisco TAC. The test log can be exported to file through the Export button located at the bottom of the Test Log (see Figure 3-15 on page 3-21). All steps displayed in the test log, including IOS CLI transcripts, are exported in text format.

Step 1 Click the **Export** button. The standard browser file download window appears with a default filename of *export.txt*.

Step 2 Save the file.

3.3 Advanced Troubleshooting Options

Advanced troubleshooting provides further options that you can use to troubleshoot your network. Advanced troubleshooting options are only available when the basic MPLS VPN Connectivity Verification test has been unable to find a failure or a failure has been found but its cause cannot be identified.

The advanced troubleshooting options supported are detailed in Table 3-8.

Table 3-8 Advanced Troubleshooting Options

Advanced Troubleshooting Option	Description
Reverse path test	Available when a failure is found but the cause of the failure is unknown.
MTU Analysis	Available when no failure is found.
LSP Visualization	Available when no failure is found.
LSP Troubleshooting	Available when an IP failure is found.

When appropriate, advanced troubleshooting options are made available through the Advanced drop-down button at the bottom of the Test Results window. In cases where no Advanced troubleshooting options are available, the Advanced button is disabled.

3.3.1 Reverse Path Testing

In some cases the MPLS VPN Connectivity Verification test detects a connectivity failure, but is unable to identify the cause of this failure. By repeating the test in the reverse direction (that is, reversing the local and remote site configuration) it might be possible to identify the cause of the problem. For example, while performing a connectivity test in the forward direction, an LSP connectivity problem might be identified on a device. However, this problem could be caused by an LDP miss-configuration on the downstream LSP neighbor. By repeating the test in the reverse direction, the miss-configured downstream router is be encountered first and the LDP miss-configuration is diagnosed. When this situation occurs, the Test Details displayed in the Test Results window advises you to perform the test in the reverse direction. The Reverse Test option is made available on the Advanced drop-down button in the Test Results window.

Selecting the Reverse Test advanced troubleshooting option invokes the MPLS VPN Connectivity Verification test in the reverse direction. No further configuration is required.

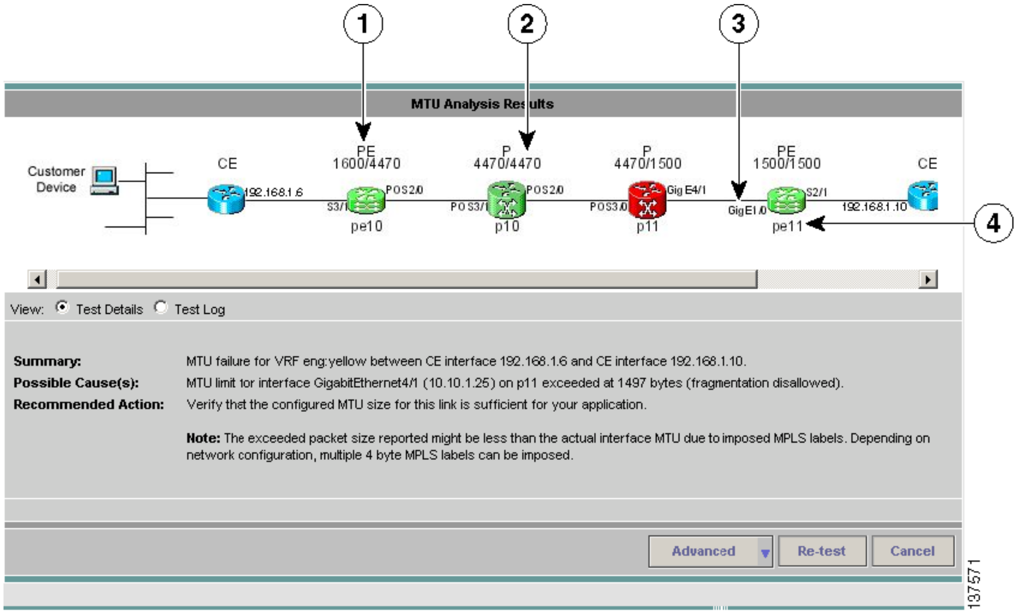
The results of the reverse path testing are displayed in the Test Results window.

3.3.2 MTU Analysis

MTU Analysis determines the minimum interface MTU size for the tested path between the local and remote sites. It then tests that packets can be successfully sent from the local site to the remote site up to the determined minimum interface MTU size and that packets are dropped at the expected constricting interface after the minimum MTU size is exceeded. This is achieved using a sweeping **ping vrf** IOS command with the *do not fragment* option set. You must interpret the MTU analysis results to determine if the configured interface MTU sizes are sufficient for your application.

While MTU Analysis is being performed, the progress window is displayed. Once complete, MTU Analysis results (see Figure 3-17) are displayed in the Test Results window.

Figure 3-17 ***Test Results Window—MTU Analysis Results***



Summary: MTU failure for VRF eng:yellow between CE interface 192.168.1.6 and CE interface 192.168.1.10.

Possible Cause(s): MTU limit for interface GigabitEthernet4/1 (10.10.1.25) on p11 exceeded at 1497 bytes (fragmentation disallowed).

Recommended Action: Verify that the configured MTU size for this link is sufficient for your application.

Note: The exceeded packet size reported might be less than the actual interface MTU due to imposed MPLS labels. Depending on network configuration, multiple 4 byte MPLS labels can be imposed.

1. Device Role (CE, PE, or P).
2. Interface MTU (ingress/egress interface).
3. IOS interface name.
4. Device hostname.

The device that enforces the constricting MTU size is highlighted in red.

The Test Details section displays details of the constricting MTU including:

- Constricting device
- Constricting interface
- Packet size at which packets start to be dropped

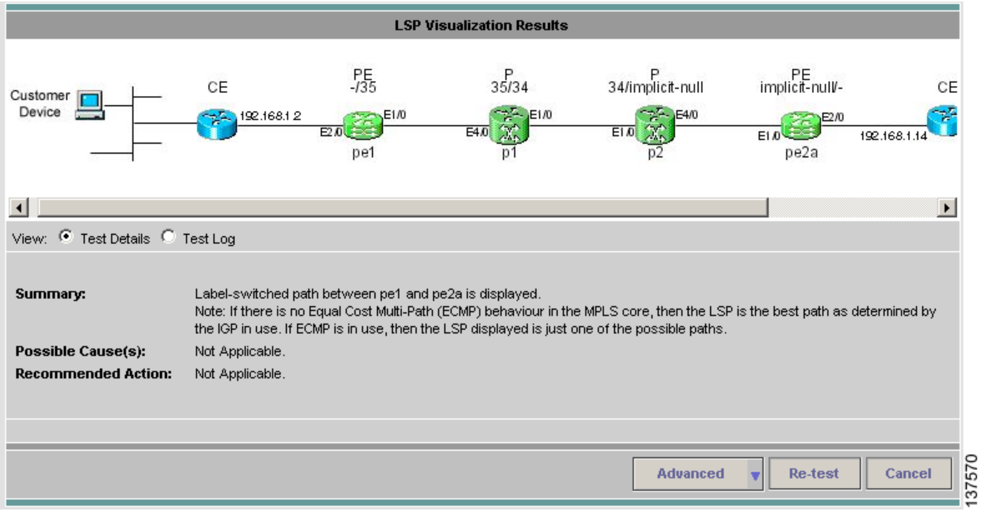
MTU analysis is only offered when an MPLS VPN Connectivity Verification test does not detect a connectivity problem.

Note The constricting interface could drop packets before they reach the interface MTU size due to MPLS labels imposed on the IP packet. The exact size depends upon the number of 4-byte MPLS labels imposed.

3.3.3 LSP Visualization

When no failure is found, the Test Results window data path displays a summary of the test performed. This does not show details of the path through the core that has been tested. LSP Visualization displays a hop-by-hop Data Path illustration of the MPLS label switched path (LSP) between the local and remote sites (see Figure 3-18). The path shown is the path tested during the MPLS VPN Connectivity Verification test.

Figure 3-18 Test Results Window—LSP Visualization



Summary: Label-switched path between pe1 and pe2a is displayed.
Note: If there is no Equal Cost Multi-Path (ECMP) behaviour in the MPLS core, then the LSP is the best path as determined by the IGP in use. If ECMP is in use, then the LSP displayed is just one of the possible paths.

Possible Cause(s): Not Applicable.

Recommended Action: Not Applicable.

The Data Path displays the following for each PE and P device in the tested path:

- Role (PE or P)
- Device name
- Interface name
- Ingress and egress labels

For more details of what is displayed in the Data Path, see 3.2.1 Data Path, page 3-17.

LSP Visualization is only offered when an MPLS VPN Connectivity Verification test does not detect a connectivity problem.

Note When using an MPLS VPN Connectivity Verification test for post-provisioning verification, LSP Visualization provides an additional level of verification by displaying the LSP path taken across the MPLS core.

3.3.4 LSP Troubleshooting

In some cases an IP failure might be found which masks an underlying LSP label problem. When an IP failure is found, the Test Results window displays details of the failure and informs the user that it might be due to an underlying LSP label problem. To eliminate possible LSP label issues, the user is advised to run LSP Troubleshooting using the Advanced button.

How Does Cisco MPLS Diagnostics Expert Work?

This chapter describes how the Cisco MPLS Diagnostics Expert application works.

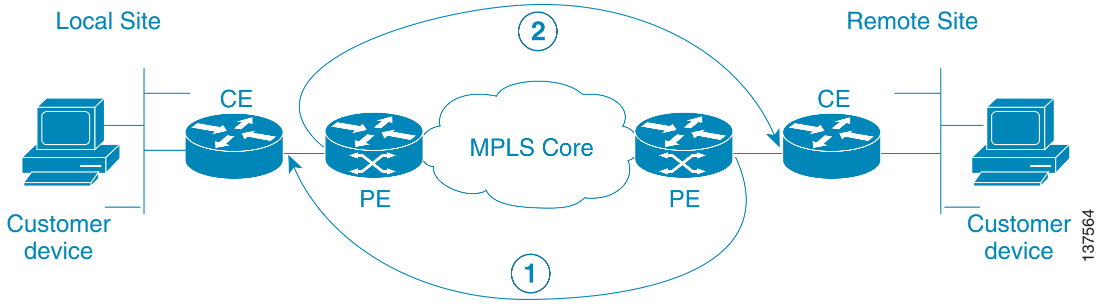
The MPLS VPN Connectivity Verification test consists of connectivity testing, troubleshooting, and diagnostics steps. The exact steps performed for each test depend upon the nature of the failure found and the location of the failure within the network. Due to the simple test configuration and result presentation, you have little need to understand the troubleshooting and diagnostics logic. However, in some cases - particularly when examining the test log - you might want an understanding of the troubleshooting and diagnostics process. This chapter provides a high-level overview of the connectivity testing, troubleshooting, and diagnostics logic.

The test scope is determined by the test configuration you enter. For example, for each site, testing could be performed to a customer device within the site, the CE access circuit interface or the PE access circuit interface. For simplicity, this chapter assumes that testing for all sites is to the CE access circuit interface.

The first step tests VPN connectivity between the two sites to determine if a problem exists. This is achieved using the Cisco IOS VRF ping functionality. Ideally this test should be initiated from a device in the local site subnet to a destination IP address in the remote site subnet. However, ISC supports managed and unmanaged Cisco CE devices, and non-Cisco CE devices. The troubleshooting and diagnostics functionality works for all cases. As a result, it is only possible to initiate tests from PE and P devices within your core network. To work around this limitation, it is necessary to perform the connectivity test in two stages (see Figure 4-1).

- The first stage tests connectivity from the remote site PE to the local site CE. This is achieved using a Cisco IOS **ping vrf** command, specifying the local site CE access circuit interface IP address as the destination and the remote site PE access circuit interface as the source IP address.
- The second stage tests connectivity from the local site PE to the remote site CE. The second stage is performed only when the **ping vrf** command in the first stage indicates successful connectivity. This is also achieved using a Cisco IOS **ping vrf** command, specifying the remote site CE access circuit interface IP address as the destination and the local site PE access circuit interface as the source IP address.

Figure 4-1 IOS VRF Ping Connectivity Tests



By testing connectivity in two stages, the troubleshooting and diagnostics functionality is able to simulate an end-to-end test from the local site CE to the remote site CE, and thus identify any VPN connectivity problems between the sites. This connectivity test exercises VPN, MPLS, and IP connectivity between the two sites.

If a VPN connectivity problem is not detected, then no troubleshooting and diagnostics are performed. If a VRF connectivity problem is detected, then a further series of connectivity tests are performed in an attempt to isolate the connectivity problem. These tests are initiated on the PE device and performed in the direction for which a VPN failure was detected. They include:

- VRF ping across core to PE access circuit interface. This determines if the failure lies on the access circuit, between the CE and PE or in the core.
- ICMP ping across core to PE loopback—This confirms that IP connectivity is working across the core.
- LSP ping across core to PE loopback—This confirms that the MPLS LSP path across the core is working.

Testing might stop at any point if the fault is isolated. A sequence of automated troubleshooting and diagnostics steps is then performed to diagnose the cause of the fault. The steps performed depend upon the nature and location of the fault. After a fault diagnosis has been made, the result is displayed in the Test Results window with appropriate recommended actions to resolve the fault. The exact connectivity testing and automated troubleshooting and diagnostics steps performed can be viewed in the Test Log section of the Test Results window.

APPENDIX A

Frequently Asked Questions

Q. When I perform an MPLS VPN Connectivity Verification Test the Progress window appears to hang and performs the same step for up to 5 minutes. After 5 minutes the Test Results window displays the following message.

```
Summary: Cannot connect or login to device router1.
Possible Cause(s): Device could be down, there could be problems with network
connectivity, or the login details in the repository might be incorrect
Recommended Action: Restore connectivity to the device before attempting the test.
If in-band network management is in use then you might want to consider performing
a Traceroute from the management station to device router1 to find where IP
connectivity fails.
```

A. The device has not responded when an attempt has been made to log on to it. Ensure that the device is not down. Ensure that you have IP connectivity from the ISC server to the device. Ensure that the device login details configured in the ISC Repository match those configured on the physical device. Ensure that all available VTY sessions on the device are not in use.

Q. When I perform an MPLS VPN Connectivity Verification Test, sometimes the devices I configured as the local site is displayed on the left hand side of the Data Path, in the Test Results window. In other instances, these local site devices are displayed at the right hand side of the Data Path, in the Test Results window. Why is this?

A. Connectivity problems in an MPLS VPN can often only be detected in a particular direction. The MPLS VPN Connectivity Verification Test tests in both directions (from local site to remote site and vice-versa). Depending on the direction of test when the problem is found, the local site devices might be displayed on either the left hand side, or right hand side of the Data Path in the Test Results window.

Q. When I perform two or more MPLS VPN Connectivity Verification tests in parallel on the same client machine, the test results for one of these tests is displayed in the Result Screens for all tests. The test results for the other tests are lost. How can I avoid this?

A. When performing parallel MPLS VPN Connectivity Verification tests on the same client machine, you must ensure each test is performed using a different HTTP session. To do so, run each test in a separate browser launched from the command line or by clicking on the browser icon on the desktop or Start menu. Do not run parallel tests in tabs within the same browser window or in browser windows launched from existing browser windows.

APPENDIX B

Unsupported Scenarios

This appendix details scenarios and technologies that are not supported by Cisco MPLS Diagnostics Expert version 1.0. For details of the features supported in Cisco MPLS Diagnostics Expert version 1.0, see 1.4 MPLS Diagnostics Expert Features, page 1-4.

B.1 IP Unnumbered Interfaces

Cisco MPLS Diagnostics Expert does not support IP unnumbered interfaces in the troubleshooting path, including the access circuit. It is tolerant of routers configured with IP unnumbered interfaces, as long as these interfaces are not in the troubleshooting path.

If an MPLS VPN Connectivity Verification Test is run on a path containing IP unnumbered interfaces, the test will abort. A pop-up dialog will display the message:

```
Errors occurred while performing the test that forced the rest of the steps to be aborted.
Please review the results for more details.
```

The Test Result window will report that the test was aborted due to unrecoverable errors.

B.2 Common PE for Local and Remote Sites

Cisco MPLS Diagnostics Expert does not support troubleshooting between sites attached to the same PE device. The MPLS VPN Connectivity Verification Configuration window will not allow you to invoke a test between two sites attached to the same PE.

The recommended workaround for this limitation is to perform a connectivity verification test from each CE to a common third CE which should be attached to a remote PE. This requires two tests to verify connectivity between CE devices sharing a common PE.

B.3 Core Tunneling Protocols

Cisco MPLS Diagnostics Expert does not support the use of tunneling protocols within the core network. This includes, but is not restricted to:

- MPLS Traffic Engineered Tunnels
- MPLS over Generic Routing Encapsulation (GRE)
- MPLS over Layer 2 Tunneling Protocol (L2TP)

B.4 Multicast VPN

Cisco MPLS Diagnostics Expert does not support Multicast VPNs.

B.5 Channelized Interfaces

Cisco MPLS Diagnostics Expert does not support the use of channelized interfaces.

INDEX

A

advanced troubleshooting options 3-22

analysis

  MTU 3-23

APIs 2-7

audience v

C

channelized interfaces B-2

Cisco

  product security overview viii

  technical support & documentation website ix

Cisco.com vii

Cisco MPLS Diagnostics Expert overview 1-1

color codes 3-17

common PE for local and remote sites B-1

configuration

  network 2-3

  using customer VPN information 3-8

core tunneling protocols B-1

creation

  manual 2-5

D

data path 3-17

definitions of service request severity x

device actions 3-18

device color codes 3-17

device configuration collection 2-7

device import 2-6

discovery 2-5

documentation vi

  feedback viii

  obtaining vii

  ordering viii

  technology-related vii

E

export 3-22

F

FAQ A-1

features 1-4

G

getting started 2-1

H

hardware supported 1-3

how does MPLS Diagnostics Expert work? 4-1

I

installing 2-2

  Cisco MPLS Diagnostics Expert 2-2

interpreting the test results 3-16

introduction 1-1

inventory 2-4

inventory manager device import 2-6

inventory requirements 2-4

inventory setup 2-4

IOS versions supported 1-3

IP unnumbered interfaces B-1

ISC

- APIs 2-7
- repository, synchronizing with device configuration 2-7

K

knowledge

- prerequisite 1-2

L

licensing 2-3

LSP

- troubleshooting 3-25
- visualization 3-24

M

manual creation 2-5

MPLS Diagnostics Expert features 1-4

MPLS VPN connectivity verification test

- performing 3-2

MTU analysis 3-23

multicast VPN B-2

N

network configuration 2-3

O

obtaining

- additional publications and information xi
- documentation vii
- technical assistance ix

ordering documentation viii

organization v

overview

- Cisco MPLS Diagnostics Expert 1-1

P

performing

- MPLS VPN connectivity verification test 3-2

preface v

prerequisite knowledge 1-2

product documentation DVD vii

progress window 3-14

R

reactive fault lifecycle 1-2

related documentation vi

reporting security problems in Cisco products ix

reverse path testing 3-23

S

security problems in Cisco products

- reporting ix

selecting

- PE access circuit interface 3-7
- PE device 3-6

setup 2-4

submitting a service request x

supported hardware and IOS versions 1-3

synchronizing

  the ISC repository with device configuration 2-7

T

technical assistance

  obtaining ix

technology-related documentation vii

terminology v

test details 3-19

testing

  central services VPN topology 3-14

  hub and spoke VPN topology 3-10

  intranet/extranet VPN topology 3-14

  reverse path 3-23

test log 3-21

test results

  interpreting 3-16

troubleshooting

  LSP 3-25

  options, advanced 3-22

U

unsupported scenarios B-1

  channelized interfaces B-2

  common PE for local and remote sites B-1

  core tunneling protocols B-1

  IP unnumbered interfaces B-1

  multicast VPN B-2

user roles 2-3

using

  Cisco MPLS Diagnostics Expert 3-1

  Cisco MPLS Diagnostics Expert workflow 3-1

  customer VPN information 3-8

V

VPN information 3-8

VPN topologies 3-10

W

workflow

  getting started 2-2

  using Cisco MPLS Diagnostics Expert 3-1