CHAPTER 57

Introduction

This chapter provides an overview of the Cisco Prime Fulfillment Diagnostics application.

This chapter contains the following sections:

Prime Diagnostics Overview

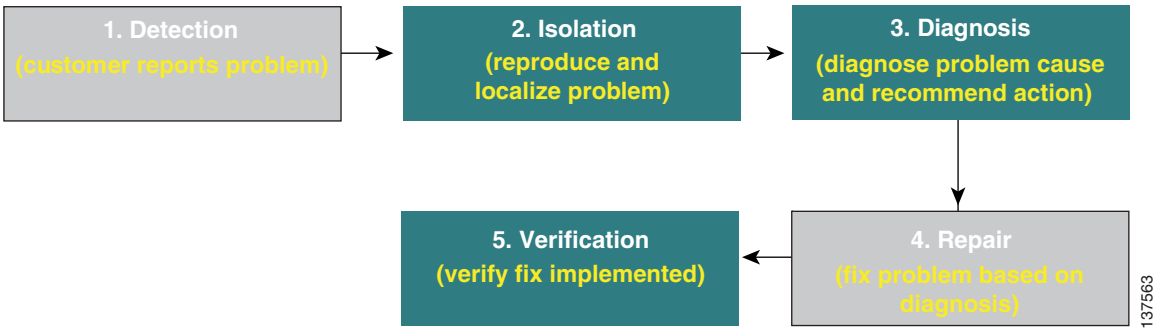
Prime Diagnostics is an automated, workflow-based network management application that troubleshoots and diagnoses problems in Multiprotocol Label Switching (MPLS) VPNs. Diagnostics offers users the capability to reduce the amount of time required to diagnose MPLS-related network outages—in many cases from hours to minutes. It performs diagnostics based on analysis of network failure scenarios, across MPLS access, edge, and core networks. It is equally applicable to both service provider and enterprise "self-deployed" MPLS VPN networks. Network operations center (NOC) support technicians as well as second-line and third-line support can benefit from this product. Diagnostics optionally integrates with the Prime Fulfillment MPLS VPN provisioning component. To diagnose MPLS VPN core problems, Cisco IOS and IOS XR software releases supporting MPLS operations and maintenance (OAM) features including label-switched path (LSP) ping and LSP traceroute are required.

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

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

Diagnostics 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 57-1. The Repair function is 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 57-1 The Reactive Fault Lifecycle



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

Diagnostics 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. Diagnostics also provides the ability to rerun 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 Prime Fulfillment (for example, VPN provisioning or Traffic Engineering Management). It can also be used in Prime Fulfillment installations where some or all of the other Prime Fulfillment 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, to locate the endpoints (for example, Customer Edge devices) between which connectivity is tested.

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

Note Diagnostics does not have any support for underlying configuration or routing changes during troubleshooting. During the execution of Diagnostics, any changes made either by the operator or through the control plane of the routers, will not be reflected in the actual troubleshooting performed. Diagnostics does not guarantee that the correct Failure Scenario or observation will be found in cases where such changes are made.

Prerequisite Knowledge

Diagnostics has been designed for use by users who have minimal MPLS VPN knowledge. A Diagnostics 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. However, due to the complex nature of MPLS VPNs, it is recommended that you will gain maximum advantage from Diagnostics 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.

Diagnostics now diagnoses Cisco devices and networks that use IETF RFC 4379 compliant Label Switched Path (LSP) ping and LSP traceroute. Diagnostics continues to support the earlier draft (draft 3) available in Cisco IOS. You must use a consistent draft of LSP ping and traceroute across all devices in your network.

Recommended reading:

- MPLS and VPN Architectures: Ivan Pepelnjak, Jim Guichard, Cisco Press
- Troubleshooting Virtual Private Networks: Mark Lewis, Cisco Press
- LSP ping/trace RFC: http://www.ietf.org/rfc/rfc4379.txt
- RFC 2547: http://www.ietf.org/rfc/rfc2547.txt?number=2547
- RFC 4379: http://www.ietf.org/rfc/rfc4379.txt?number=4379
- MPLS Embedded Management—LSP Ping/Traceroute and AToM VCCV: http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/gslsppt.html

Supported Hardware, IOS, and IOS XR Versions

For details of Provider (P) and Provider Edge (PE) network device types and related Cisco IOS and IOS XR versions supported, see the *Cisco Prime Fulfillment Installation Guide 6.1.*

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

Device types, IOS, and IOS XR versions detailed in the Chapter 7, "Setting Up the Prime Fulfillment Services" support the MPLS label switched path (LSP) Ping and Traceroute feature. This feature is required for Diagnostics troubleshooting. If all P and PE devices comply with the list of supported device types, IOS, and IOS XR versions, Diagnostics can troubleshoot access circuit, MPLS VPN, and MPLS core problems. Diagnostics is tolerant to other device types, IOS, and IOS XR 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 57-1 shows the possible scenarios and likely outcome.

Table 57-1 Hardware, IOS, and IOS XR Version Compliance

Scenario	Outcome
All P and PE devices comply with the supported Cisco hardware, IOS, and IOS XR 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, IOS, and IOS XR versions. One or more P device(s) do not comply with the supported Cisco hardware, IOS, and IOS XR 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 devices are Cisco hardware running unsupported IOS and IOS XR versions that do not support the MPLS LSP Ping and Traceroute feature.	MPLS VPN Connectivity Verification test *may* be able to successfully troubleshoot access circuit and MPLS VPN issues. The MPLS VPN Connectivity Verification test is unable to perform troubleshooting of the MPLS core.
PE devices are non-Cisco hardware.	MPLS VPN Connectivity Verification test cannot be run.

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

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

Note If the PE devices are running unsupported IOS or IOS XR versions, that do not implement the MPLS Ping and Traceroute features, access circuit and VPN edge troubleshooting is performed, but no troubleshooting of the MPLS core is possible. In this scenario some core failures are reported as a Label Forwarding Information Base (LFIB) mismatch on a PE device. The LFIB mismatch is a symptom of the core failure, but the actual core failure cannot be diagnosed because core troubleshooting is not possible.

IPv6

The IPv4 address free pool held by the Internet Assigned Numbers Authority (IANA) is running out. Cisco is addressing this shortage by adopting IPv6 addressing.

Diagnostics supports configuration and selection of devices with both IPv4 and IPv6 addresses. Diagnostics can troubleshoot MPLS VPN services where the attachment circuits:

- use IPv6 addressing
- use dual stack IPv4/IPv6 addressing.

Dual stack is a technique that allows both IPv4 and IPv6 to coexist on the same interfaces. For many years, if not forever, there will be a mix of IPv6 and IPv4 nodes on the Internet. Thus compatibility with the large installed base of IPv4 nodes is crucial for the success of the transition from IPv4 to IPv6. For example, a single interface can be configured with an IPv4 address and an IPv6 address. All the elements referenced as dual-stacked, such as provider edge and customer edge routers, run IPv4 as well as IPv6 addressing and routing protocols.

Note Diagnostics supports only global unicast IPv6 addresses. A global unicast address is very similar in function to an IPv4 unicast address such as 131.107.1.100. In other words, these addresses are conventional and publicly routable addresses. A global unicast address includes a global routing prefix, a subnet ID, and an interface ID.

Table 57-2 General Unicast Address Structure

Fields	Network prefix	Subnet	Interface Identifier
Bits	48	16	64

Note Diagnostics permits to launch a test where both attachment circuit endpoints are either IPv6 and IPv6 or IPv4 and IPv4. No mixed addressing formats can be specified

For more details about when a test is initiated on an IPv6 address, see Chapter 59, “Understanding the Diagnostics Connectivity Tests”.

Diagnostics Features

Diagnostics troubleshooting and diagnostics supports the following four domains:

- Access Circuit—Access circuit troubleshooting includes basic routing protocol troubleshooting, basic layer 1 and layer 3 troubleshooting, and advanced layer 2 troubleshooting for ATM, Frame Relay, and Ethernet.
- MPLS VPN—MPLS VPN troubleshooting supports MPLS/MP-BGP VPNs based on RFC2547. The following topologies are supported: hub and spoke, central services, full mesh, and intranet or extranet VPN.
- MPLS Core—MPLS core troubleshooting supports data plane and control plane diagnostics. This is provided for all MPLS core and edge devices (including troubleshooting of any discovered MPLS Traffic Engineered Tunnels) running a Cisco IOS or Cisco IOS XR version with MPLS Operation, Administration, and Maintenance (OAM) support. For details of Cisco IOS, and Cisco IOS XR versions with MPLS OAM support, see the "Supported Hardware, IOS, and IOS XR Versions" section on page 57-3.

Note Diagnostics does not troubleshoot routing protocols within the core (except OSPF failures on first hop and PE-P-PE topology if the IGP protocol is OSPF), IP connectivity within the core, and some variants of inter-Autonomous Systems (AS) or Carrier-Supporting-Carrier (CsC), specifically Inter AS option B and CsC where there is no LSP.