



CHAPTER 11

Performing Diagnostics

This chapter describes the Diagnostics application in Cisco Prime Provisioning 6.3.

Introduction

This section provides an overview of the Cisco Prime Provisioning Diagnostics application.

The chapter contains the following sections:

- [Diagnostics Overview, page 11-1](#)
- [Prerequisite Knowledge, page 11-2](#)
- [Supported Hardware, IOS, and IOS XR Versions, page 11-3](#)
- [IPv6, page 11-4](#)
- [Diagnostics Features, page 11-5](#)

Diagnostics Overview

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 Provisioning 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 11-1](#). 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 11-1 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 Provisioning (for example, VPN provisioning or Traffic Engineering Management). It can also be used in Prime Provisioning installations where some or all of the other Prime Provisioning 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 Provisioning 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 Provisioning 6.3 Installation Guide*.



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](http://www.cisco.com).

Device types, IOS, and IOS XR versions detailed in [Setting Up the Prime Provisioning Services, page 3-6](#) 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 11-1](#) shows the possible scenarios and likely outcome.

Table 11-1 **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.

Table 11-1 *Hardware, IOS, and IOS XR Version Compliance (continued)*

Scenario	Outcome
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 <i>may</i> 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 11-2 *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 [Understanding the Diagnostics Connectivity Tests, page 11-14](#).

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 11-3](#).

**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.

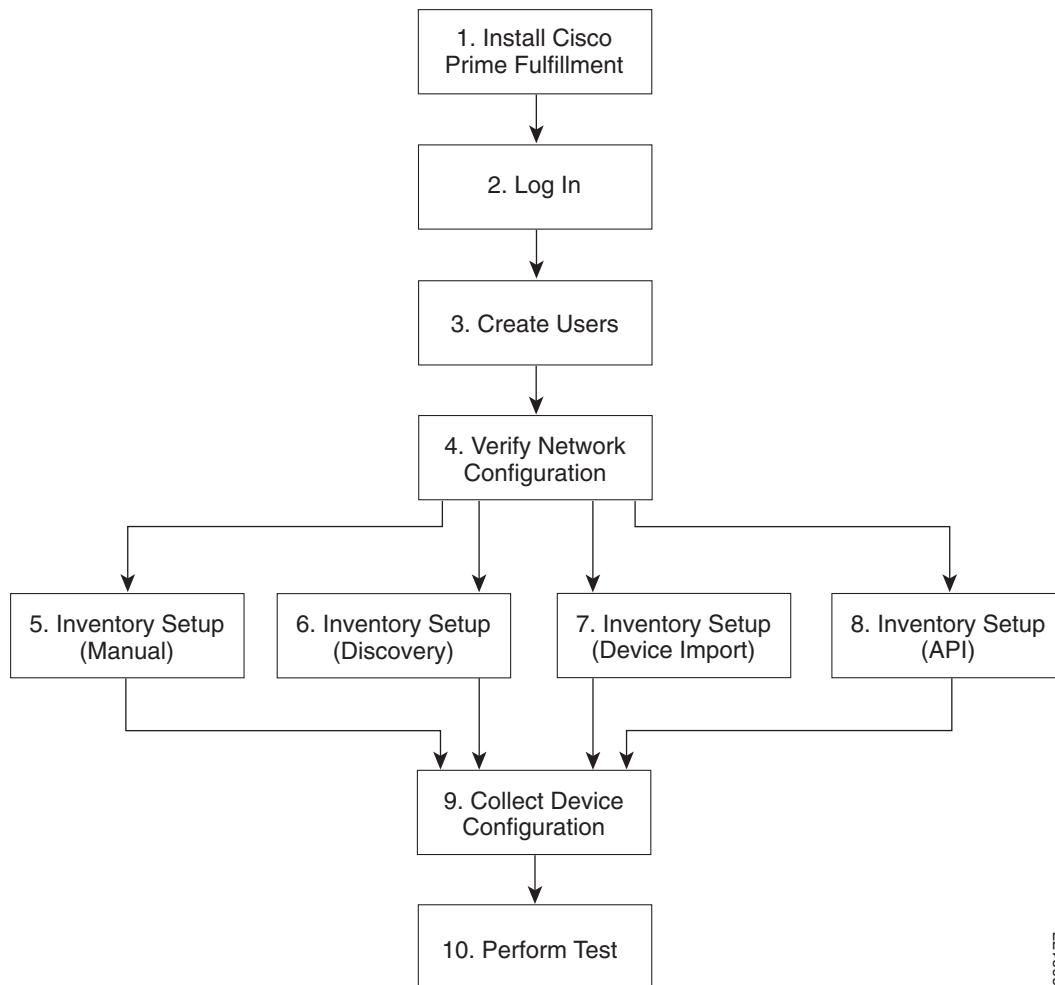
Getting Started

This section describes how to get started using Cisco Prime Provisioning Diagnostics.

It contains the following sections:

- [User Roles, page 11-7](#)
- [User Roles, page 11-7](#)
- [Creating Users, page 11-7](#)
- [Network Configuration, page 11-7](#)
- [Inventory Setup, page 11-8](#)

[Figure 11-2](#) describes the getting started workflow for Diagnostics.

Figure 11-2 *Getting Started with Diagnostics*

282177

6. Create Users—Create users and assign Diagnostics user roles. See [User Roles, page 11-7](#), and [Creating Users, page 11-7](#).
7. Verify Network Configuration—Verify that all network devices have the configuration required for Diagnostics. See [Network Configuration, page 11-7](#).
8. Inventory Setup (Manual)—Manually create required Prime Provisioning inventory objects. See [Inventory Setup, page 11-8](#).
9. Inventory Setup (Discovery)—Create required Prime Provisioning inventory objects using Prime Provisioning Discovery. See [Inventory Setup, page 11-8](#).
10. Inventory Setup (Device Import)—Create required Prime Provisioning inventory objects using Inventory Manager Import Devices feature. See [Inventory Setup, page 11-8](#).
11. Inventory Setup (API)—Create required inventory objects through Prime Provisioning APIs. See [Inventory Setup, page 11-8](#).
12. Collect Device Configuration—Collect device configuration, including interface configuration, and add to Prime Provisioning inventory. A scheduled task can be set up to periodically synchronize Prime Provisioning inventory with actual device configuration. See [Device Configuration Collection, page 11-11](#).

13. Perform Test—Select, configure, and run an MPLS VPN Connectivity Verification test. See [Performing an MPLS VPN Connectivity Verification Test, page 11-18](#).

User Roles

The functionality available to you as an Prime Provisioning user is determined by your assigned user roles. User roles also allow you to create and delete devices, collect device configuration, and to perform an MPLS VPN Connectivity Verification test.

To use the Diagnostics functionality, you must be assigned one or more of the following predefined Diagnostics roles depending on the type of connectivity tests you are entitled to perform:

1. **MplsDiagnosticsRole**—You can perform an MPLS VPN connectivity test between two CEs.
2. **MplsDiagnosticsPeToAttachedCeTestRole**—You can perform an MPLS VPN connectivity test between a PE and an attached CE.
3. **MplsDiagnosticsCetoPeAcrossCoreTestRole**—You can perform an MPLS VPN connectivity test between a CE and a PE across the MPLS core.
4. **MplsDiagnosticsPetoPeInVrfTestRole**—You can perform an MPLS VPN connectivity test between two PEs.
5. **MplsDiagnosticsPeToPeCoreTestRole**—You can perform a core MPLS connectivity test between two PEs.



Note

All Diagnostics roles allow you to create and delete devices, collect device configuration, and to perform an MPLS VPN Connectivity Verification test.

Creating Users

For details on how to create Prime Provisioning users, see [Cisco Prime Provisioning 6.3 Administration Guide](#).

Network Configuration

This section describes the network configuration required to allow Diagnostics to troubleshoot your network.

MPLS IP Time To Live Propagation

MPLS IP Time To Live (TTL) propagation is enabled by default on Cisco devices. Diagnostics requires that MPLS IP TTL propagation is enabled within the MPLS core. If MPLS IP TTL propagation is not enabled, then Diagnostics 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.

In Cisco IOS, it is possible to disable MPLS IP TTL propagation for packets forwarded to the MPLS core by using the **no mpls ttl-propagate forward** IOS command. This command stops TTL propagation for packets forwarded in to the MPLS core, but allows TTL propagation for packets sent from within the MPLS core. Diagnostics functions correctly in this situation.

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

**Note**

Timestamp must be disabled for the devices, that are selected for troubleshooting and as well as for the devices that are part of the same network.

MPLS LSP Ping/Trace Route Revision

Diagnostics supports IOS MPLS LSP Ping/Traceroute implementations based on version 3 of the IETF LSP Ping draft (draft-ietf-mpls-lsp-ping-03.txt). Later versions of the IETF LSP Ping draft are not supported. Recent IOS versions (including 12.4(6)T), and IOS XR implement later versions of the IETF LSP Ping draft / RFC 4379. To use Diagnostics with these IOS or IOS XR versions you must configure IOS or IOS XR to use version 3 of the IETF LSP Ping draft. To do so you should enter the **mpls oam** command followed by the **echo revision 3** command in IOS or IOS XR global configuration mode. You should ensure that all routers in your core are using the same version of the IETF LSP ping draft or RFC as appropriate.

31-Bit Prefixes on Point-to-Point Access Circuit Links

For Access circuit links that use IPv4 addressing, Diagnostics supports troubleshooting over access circuit links configured with a 31-bit prefix. However, for each classful network, Diagnostics does not support troubleshooting over two possible 31-bit prefix configurations. These are the subnets that use the classful network address or network broadcast address as a host address. For example, in the class A network, 10.0.0.0, the 31-bit prefix subnet that uses the IP addresses 10.0.0.0 and 10.0.0.1 as host addresses, and the subnet that uses the IP addresses 10.255.255.254 and 10.255.255.255 as host addresses, are not supported. All subnets between these ranges are supported.

If a Diagnostics test is configured using an unsupported 31-prefix subnet, then the test is not run and a message is displayed informing you of the unsupported 31-bit prefix configuration. In this situation, you must manually troubleshoot this link or reconfigure the link to use a supported subnet configuration.

Inventory Setup

Diagnostics can be used without any dependency on other Prime Provisioning modules. However, before it can be used, the Prime Provisioning 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 Prime Provisioning is a logical representation of a physical device in the network. Every network element that Prime Provisioning 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 and then assigned a PE Device type.

All Provider Edge (PE) and Provider (P) routers in the MPLS network must be added to the Prime Provisioning 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 Prime Provisioning 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 Prime Provisioning inventory. A Route Reflector should be added as a Device and then as a PE Device with role type of P. By adding the Route Reflector to the Prime Provisioning inventory, Diagnostics is able to identify possible failures involving this device.

**Note**

If other Prime Provisioning features are being used to manage the MPLS network, many of the required inventory objects might already exist. For example, if the Prime Provisioning 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 Prime Provisioning GUI, using the Prime Provisioning Discovery functionality, using the Inventory Manager Import Devices functionality, or using third-party Operations Support System (OSS) client programs that utilize the Prime Provisioning APIs. Each of these options is described in the following sections:

- [Manual Creation, page 11-9](#)
- [Discovery, page 11-10](#)
- [Inventory Manager Device Import, page 11-10](#)
- [Prime Provisioning APIs, page 11-11](#)
- [Prime Provisioning APIs, page 11-11](#)

**Note**

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

Manual Creation

Manual creation allows you to add objects to the Prime Provisioning Repository by entering the required configuration through the Prime Provisioning Graphical User Interface (GUI). Manual object creation is recommended where a small number of objects are being added to the Prime Provisioning 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 Prime Provisioning 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 [Inventory Setup, page 11-8](#). When selecting the transport mechanism to be used between the Prime Provisioning server and the device, Cisco CNS Configuration Engine cannot be used with Diagnostics as it does not support the necessary commands that Diagnostics requires. If attempts are made to use Cisco CNS Configuration Engine with Diagnostics, then Diagnostics incorrectly reports that the device cannot be contacted.

For details of how to manually create Provider, Provider Region, Device and PE Device objects, see [Setting Up Resources, page 2-40](#).

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 [Device Configuration Collection, page 11-11](#). We recommend that you use a Collect Configuration task.

Discovery

Discovery allows you to add the devices in your network to the Prime Provisioning Repository by configuring minimal device and topology information in XML files. The Discovery process then queries these devices and populates the Prime Provisioning 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.

Prime Provisioning Discovery provides two methods for discovering devices: CDP or Device/Topology. Before performing Device Discovery it is necessary to create the required Discovery XML configuration files. For details of how to discover devices, see [Appendix E, “Inventory - Discovery.”](#)

**Note**

Both Provider (P) and Provider Edge (PE) devices should be added to the Prime Provisioning 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 [Inventory Setup, page 11-8](#).

**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, Diagnostics 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 [Device Configuration Collection, page 11-11](#).

Inventory Manager Device Import

The Inventory Manager Import Devices feature allows you to import multiple devices in to the Prime Provisioning 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 [Appendix E, “Inventory - Discovery.”](#)

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 [Appendix E, “Inventory - Discovery.”](#)

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 Prime Provisioning server.

**Note**

Both Provider (P) and Provider Edge (PE) devices should be added to the Prime Provisioning 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 [Inventory Setup, page 11-8.](#)

**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 in to the Prime Provisioning 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 Prime Provisioning Repository. If both the enable and enable secret passwords are set for a device, the Inventory Manager Import Devices feature uses the enable password for the device added to the Prime Provisioning Repository. You must override this password with the correct enable secret password. The enable password for devices in the Prime Provisioning 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, Diagnostics is unable to log in to the imported devices to perform troubleshooting. For details of how to perform a Task Manager Collect Configuration task, see [Device Configuration Collection, page 11-11.](#)

Prime Provisioning APIs

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

**Note**

The Prime Provisioning API is not included as standard with Diagnostics, it can be purchased separately.

For details of how to use the Prime Provisioning APIs, see the [Cisco Prime Provisioning 6.3 API Programmer Guide](#) and the [Cisco Prime Provisioning API 6.3 Programmer Reference](#).

Device Configuration Collection

We recommend that a Task Manager Collect Configuration task is used to add interface configuration to Devices in the Prime Provisioning 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 Prime Provisioning Repository with this information.

For details of how to add Device interface configuration using a Task Manager Collect Configuration task, see [Task Manager, page 10-23](#).

Synchronizing the Prime Provisioning Repository with Device Configuration



Note

The accuracy of Diagnostics is dependent on up-to-date device information. We recommend that the device configuration is resynchronized with the physical devices after any configuration changes and at periodic intervals. This ensures that the device configuration held in the Prime Provisioning 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 task. Either Collect Configuration or Collect Configuration from File can be used. For details of how to create a scheduled Task Manager Collect Configuration task, see [Task Manager, page 10-23](#). All PE and P 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. We recommend running the Task Manager Collect Configuration task daily on each P and PE router.

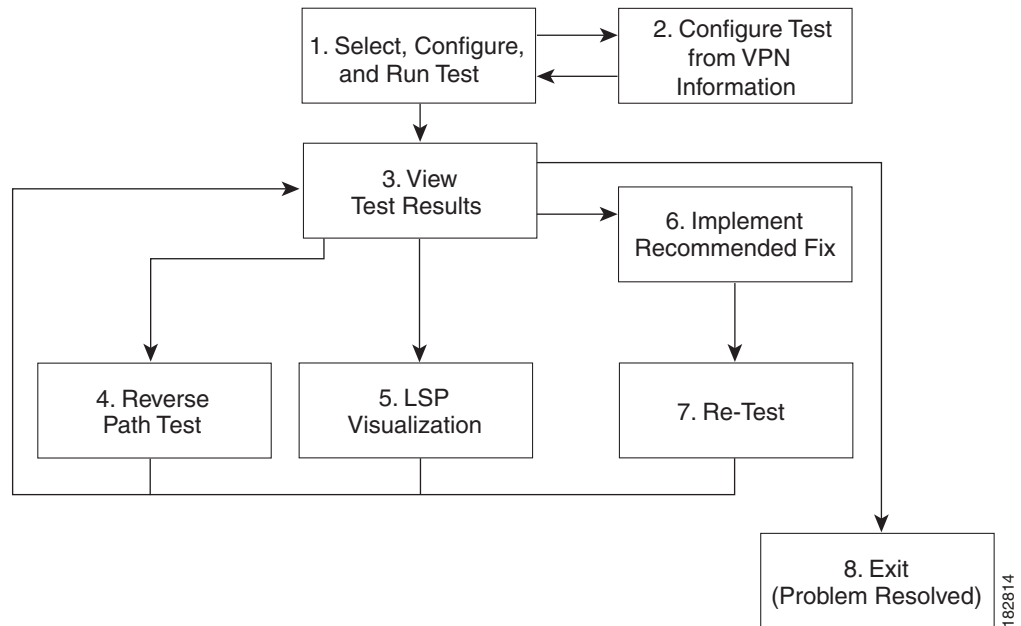
Using Cisco MPLS Diagnostics Expert

This section describes how to use Diagnostics.

It contains the following sections:

- [Understanding the Diagnostics Connectivity Tests, page 11-14](#)
- [Performing an MPLS VPN Connectivity Verification Test, page 11-18](#)
- [Progress Window, page 11-37](#)
- [Interpreting the Test Results, page 11-37](#)
- [Advanced Troubleshooting Options, page 11-43](#)
- [Switching Tunnel Checking Off—For Networks with Non-Cisco P Routers, page 11-46](#)

[Figure 11-3](#) describes the workflow for using Diagnostics.

Figure 11-3 **Using Diagnostics Workflow**

182814

1. Select, Configure, and Run Test—Configure and run an MPLS VPN Connectivity Verification test. See [Performing an MPLS VPN Connectivity Verification Test, page 11-18](#).
2. Configure Test from VPN Information—Optionally configure an MPLS VPN Connectivity Verification test using VPN information. This is only possible if Prime Provisioning VPN Provisioning functionality is used to provision VPNs within the network. See [Configuring Using Customer VRF Information, page 11-27](#) and [Configuring Using Customer VPN/VRF Information, page 11-29](#).
3. View Test Results—View results of MPLS VPN Connectivity Verification test, including the Test Log. See [Interpreting the Test Results, page 11-37](#).
4. Reverse Path Test—Perform Reverse Path Test advanced troubleshooting. See [Reverse Path Testing, page 11-44](#).
5. LSP Visualization—Perform LSP Visualization advanced troubleshooting. See [LSP Visualization, page 11-44](#).
6. Implement Recommended Fix—Manually implement fix as recommended by test results.
7. Retest—Rerun the MPLS VPN Connectivity Verification test. This would typically be done to verify the fix implemented.

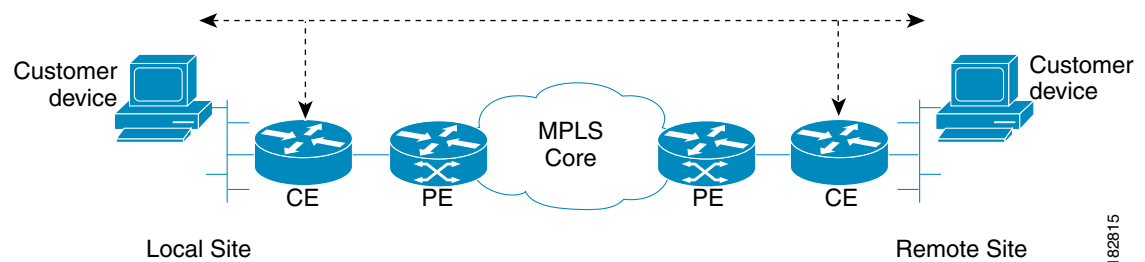
Understanding the Diagnostics Connectivity Tests

The connectivity tests are designed to troubleshoot subsections of the overall CE to CE network. The provided connectivity tests are as follows:

1. L3VPN - CE to CE—Checks the MPLS VPN connectivity between two CEs. See [L3VPN - CE to CE Connectivity Test, page 11-14](#)
2. L3VPN - PE to attached CE—Checks the MPLS VPN connectivity between a PE and the attached CE. See [L3VPN - PE to Attached CE Connectivity Test, page 11-15](#)
3. L3VPN - CE to PE across Core—Checks the MPLS VPN connectivity between a CE and a PE across the MPLS core. See [L3VPN - CE to PE Across Core Connectivity Test, page 11-16](#)
4. L3VPN - PE to PE (in VRF)—Checks the MPLS VPN connectivity between two PEs. See [L3VPN - PE to PE in VRF Connectivity Test, page 11-16](#)
5. MPLS - PE to PE —Checks the MPLS Core connectivity between two PEs. See [L3VPN - PE to PE Connectivity Test, page 11-17](#)

L3VPN - CE to CE Connectivity Test

The L3VPN - CE to CE test ([Figure 11-4](#)) checks the MPLS VPN connectivity between two CEs or Customer devices where the Customer device IP address is known.

Figure 11-4 L3VPN - CE to CE Connectivity Test

182815

Diagnostics performs core, edge, and attachment circuit troubleshooting in this case.

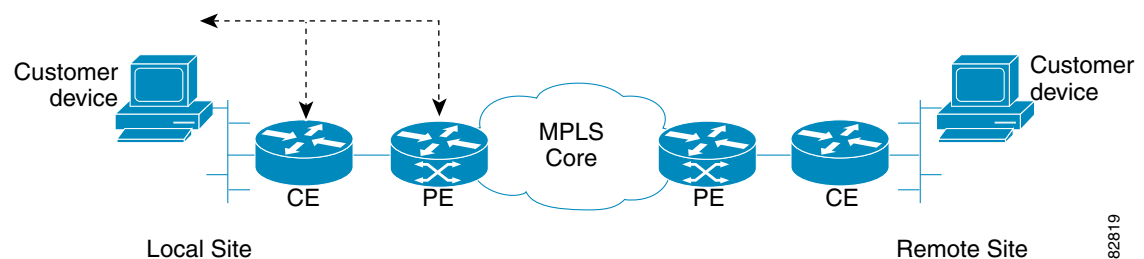
IPv6 troubleshooting

A L3VPN - CE to CE test launches troubleshooting on the IPv6 segment when all the following conditions are met:

- If a row with global unicast IPv6 address is selected from the interface selection screen or if the specified local and remote PE access circuit interfaces are having a global unicast IPv6 address or when the interface details are not available in the database.
- If the specified CE access circuit interface IP address for both local and remote-site is a global unicast IPv6 address.
- Optionally, if the specified customer device IP address for both local and remote site or for local or remote site is a global unicast IPv6 address.

L3VPN - PE to Attached CE Connectivity Test

The L3VPN - PE to attached CE connectivity test (Figure 11-5) performs a VPN connectivity test between a PE and the locally attached CE. Diagnostics performs edge and attachment circuit troubleshooting in this case.

Figure 11-5 L3VPN - PE to Attached CE Connectivity Test

182819

The L3VPN - PE to attached CE connectivity test cannot be run in the reverse direction.

The local attachment circuit is often responsible for a connectivity failure. You can test the local attachment circuit on its own, without requiring remote site PE and CE details that might not be available.

The L3VPN - PE to attached CE connectivity test allows you to diagnose the same attachment circuit connectivity outage reported by a VRF-aware IP SLA probe. The notification has all the information required to set up the corresponding access circuit connectivity test in Diagnostics.

IPv6 troubleshooting

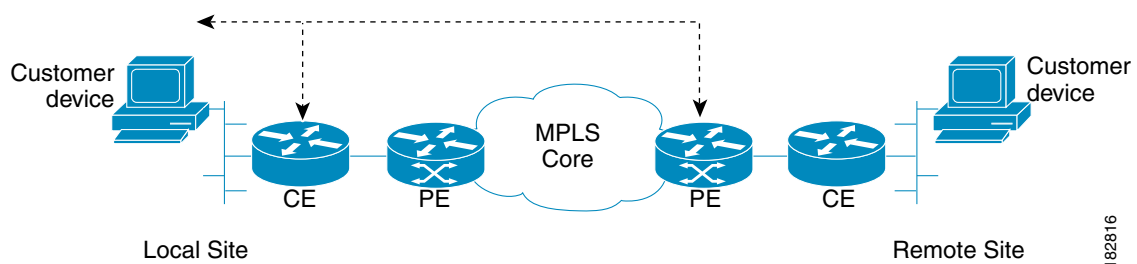
A L3VPN - PE to attached CE test launches troubleshooting on the IPv6 segment when all the following conditions are met:

- If a row with global unicast IPv6 address is selected from the interface selection screen or if the specified PE access circuit interface is having a global unicast IPv6 address or when the interface details are not available in the database.
- If the specified CE access circuit interface IP address is a global unicast IPv6 address.
- Optionally, if the specified Customer device IP address is a global unicast IPv6 address.

L3VPN - CE to PE Across Core Connectivity Test

The L3VPN - CE to PE across core connectivity test (Figure 11-6) checks the MPLS VPN connectivity between a CE or Customer devices (where the Customer device IP address is known), and a PE across the MPLS core.

Figure 11-6 L3VPN - CE to PE Across Core Connectivity Test



Diagnostics troubleshoots the core, both edges, and the attachment circuit in this case.

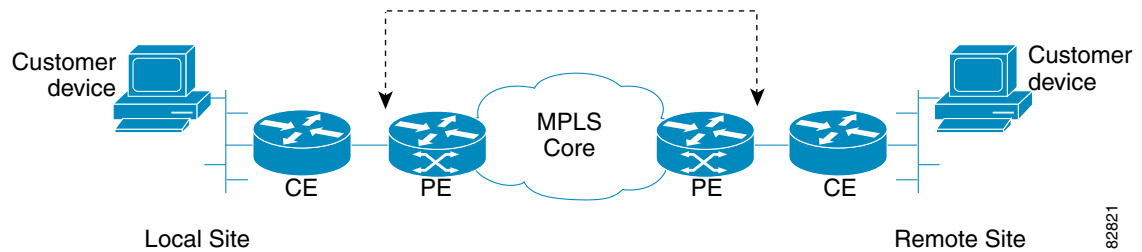
IPv6 troubleshooting

A L3VPN - CE to PE across core test launches troubleshooting on the IPv6 segment when all the following conditions are met:

- If a row with global unicast IPv6 address is selected from the interface selection screen or if the specified PE access circuit interface is having a global unicast IPv6 address or when the interface details are not available in the database.
- If the specified CE access circuit interface IP address is a global unicast IPv6 address.
- Optionally, if the specified customer device IP address is a global unicast IPv6 address.
- If the selected or specified PE access circuit interface is having a global unicast IPv6 address or when the interface details are not available in the database.

L3VPN - PE to PE in VRF Connectivity Test

The L3VPN - PE to PE in VRF connectivity test (Figure 11-7) checks the MPLS VPN connectivity between two PEs. Diagnostics troubleshoots the core and the edge on both sides.

Figure 11-7 L3VPN - PE to PE in VRF Connectivity Test

Some organizations provision the core or edge network but do not immediately allocate CEs. The L3VPN - PE to PE connectivity in VRF test allows you to deploy and test your network in phases. This test option also provides more flexibility and allows the edge or core network segment to be tested when CE information is not readily available.

The L3VPN - PE to PE connectivity in VRF connectivity test also allows you to diagnose the same short reach (PE to remote PE) VPN connectivity outage reported by a VRF-aware IP SLA probe. The notification has all the information to set up the corresponding edge connectivity test in Diagnostics.

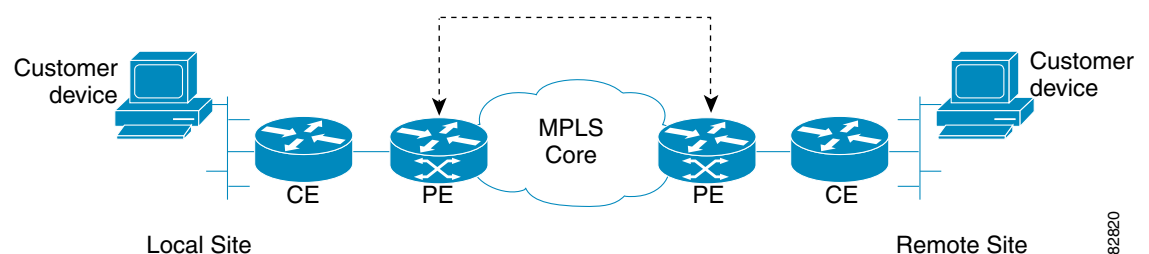
IPv6 troubleshooting

A L3VPN - PE to PE in VRF test launches troubleshooting on the IPv6 segment when all the following conditions are met:

- Either the local site PE access circuit interface or the remote site PE access circuit interface with global unicast IPv6 address needs to be selected from the interface selection screen.
- If a row with global unicast IPv6 address is selected from the interface selection screen or if the specified local PE access circuit interface is having only a global unicast IPv6 address.
- If a row with global unicast IPv6 address is selected from the interface selection screen or if the specified remote PE access circuit interface IP address is having only a global unicast IPv6 address.

L3VPN - PE to PE Connectivity Test

The L3VPN - PE to PE core connectivity test ([Figure 11-8](#)) checks the MPLS connectivity between two PEs.

Figure 11-8 L3VPN - PE to PE Core Connectivity Test

The L3VPN - PE to PE core test is intended for cases where there is blocked access to the CE interface, such as using an access list, or cases where different groups within an organization are responsible for different network segments. For example, a Core group might have a P issue but does not have the end customer context to perform a full CE-CE or PE-PE test.

The L3VPN - PE to PE core test allows you to diagnose the same core connectivity outage reported by IP SLA Health monitor probes testing connectivity between MPLS enabled PEs. The notification has all the information to set up the corresponding core connectivity test in Diagnostics.

IPv6 troubleshooting

In case of a L3VPN - PE to PE in core test, an IPv6 troubleshooting cannot be initiated as this test type uses only the IPv4 address.

Performing an MPLS VPN Connectivity Verification Test

This section describes how to perform an MPLS VPN Connectivity Verification test. This section contains the following information:

- [Opening the MPLS Diagnostics Expert Feature Selection Window, page 11-18](#)
- [Selecting, Configuring, and Running a L3VPN - CE to CE Test, page 11-19](#)
- [Selecting, Configuring, and Running a L3VPN - PE to Attached CE Test, page 11-30](#)
- [Selecting, Configuring, and Running a L3VPN - CE to PE Across Core Test, page 11-31](#)
- [Selecting, Configuring, and Running a L3VPN - PE to PE Test, page 11-32](#)
- [Selecting, Configuring, and Running a MPLS - PE to PE Test, page 11-33](#)



Note

For every command executed on a device with IOS XR version 3.8.0 or onwards, the first line of the output shows the current time stamp of the device, which Diagnostics fails to handle. The *timestamp disable* command should be used to disable the time stamp on XR devices before launching a test.

Opening the MPLS Diagnostics Expert Feature Selection Window



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 Log in to Prime Provisioning. For details of how to log in, see the [Cisco Prime Provisioning 6.3 Installation Guide \(Installing and Logging Into Prime Provisioning > Logging In for the First Time\)](#).

The Prime Provisioning home window appears.

Step 2 Click the Diagnostics tab.

The MPLS Diagnostics Expert Feature Selection window displaying the available MPLS VPN connectivity verification test types appears.



Note

You must check that you have at least one Diagnostics user role assigned to you, see [User Roles, page 11-7](#).

**Note**

The tests types available to you are determined by your assigned user roles. A user role must be defined for each test type. If you do not have access to a test type, that test type does not appear on the MPLS Diagnostics Expert Feature Selection window. See [User Roles, page 11-7](#) for further information.

Selecting, Configuring, and Running a L3VPN - CE to CE Test

This section details how to select, configure, and run a L3VPN - CE to CE test type.

Step 1 From the Diagnostics menu, select the L3VPN - CE to CE test type.

Step 2 Click on the L3VPN - CE to CE connectivity verification test type.

See [L3VPN - CE to CE Connectivity Test, page 11-14](#) for information on L3VPN - CE to CE connectivity verification test type. The L3VPN - CE to CE window appears displaying the input window corresponding to the L3VPN - CE to CE test type.

**Tip**

Each available test type has its own input window and requests a different sets of parameters, for example, the L3VPN - CE to CE test requires information for both the local and the remote sites, while the test set up window for a L3VPN - PE to attached CE test only requires local site details.

Figure 11-9 L3VPN - CE to CE Test Type

L3VPN - CE to CE

Test Representation

Local Site Find by VRF

PE Device Name *	Select	
PE Access Circuit Interface *	Select	
CE Access Circuit Interface IP Address * ¹	<input type="checkbox"/> Pings Ignored	
Customer Device IP Address:		

Remote Site Find by VRF

PE Device Name *	Select	
PE Access Circuit Interface *	Select	
CE Access Circuit Interface IP Address * ¹	<input type="checkbox"/> Pings Ignored	
Customer Device IP Address:		

Find by Service Clear Run

Note: * - Required Field
 Note: *¹ - Optional - if the Access Circuit is a /30 or /31 subnet [only for IPv4]
 Note: * - To launch troubleshooting on 6VPE

- Select or specify PE Access Circuit Interface with IPv6 address
- Specify a Global Unicast IPv6 address for the CE Access Circuit Interface IP Address
- Optional - Specify a Global Unicast IPv6 Address for the Customer Device IP Address

238852

The L3VPN - CE to CE window allows you to configure the connectivity test you would like to perform. This window displays the following components:

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

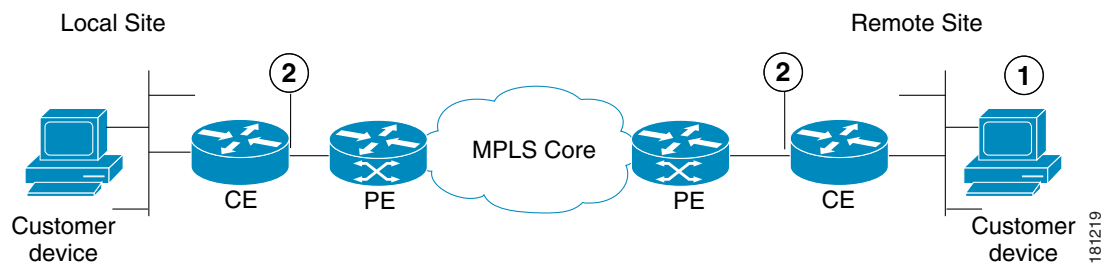
The network diagram is a static image that provides you with context for the information you must enter to configure the test.

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 can be tested in both directions.

The scope of the L3 VPN connectivity test (see [Figure 11-10](#)) can be changed on a per-site basis. For each site you can test connectivity to a customer device within the site (shown in [Figure 11-10](#) as 1), or to the CE access circuit interface (shown in [Figure 11-10](#) as 2). The test scope is determined by the configuration that you provide.

Where the IP address of a customer device is known, it might be desirable to perform a connectivity verification test to that device. Where the IP address of a customer device is not known, the connectivity verification test can be performed to the CE for the site.

Figure 11-10 Test Scope



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

To test connectivity to a device within the customer site subnetwork, you should enter the IP address of the device in the Customer Device IP Address field. 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 L3VPN - CE to CE Diagnostics - Test Setup window. You are unable to continue until all required fields have been completed with valid information.



Note

Diagnostics automatically populates the CE Access Circuit Interface IP Address field if /30 or /31 addressing is used.

Cisco IOS and Cisco IOS XR Access Control Lists (ACL) 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 reports 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 Pings Ignored check box should be checked for that site. This allows Diagnostics to take account the blocking access ACL when troubleshooting and therefore return a more accurate diagnosis of any problem found.



Note When checking the Pings Ignored check box for a site, the CE IP address and optionally the Customer Device IP Address field are used to perform troubleshooting and configuration checks on the PE device.

Step 3 Configure the fields in the L3VPN - CE to CE window as required.

Table 11-3 provides field descriptions of the L3VPN - CE to CE window.



Note The fields displayed depend on the type of test you selected, for example, the CE to CE test requires information for both the local and the remote sites, while the test set up window for a PE to attached CE test only requires local site details.



Note An alternative way to configure the test is to use customer VPN information. See [Configuring Using Customer VPN/VRF Information](#), page 11-29 for further information.

Table 11-3 Field Descriptions for the L3VPN - CE to CE Diagnostics - Test Setup Window

Field	Valid for Test Type	Description
Find by VRF	All	Click the Find by VRF button to configure the test using PE hostname or PE interface details identified using a VRF search. (See the “Configuring Using Customer VRF Information” section on page 11-27.)
PE Device Name	All	<p>Enter the site PE Device Name in the PE Device Name field or select the site PE Device Name by clicking the Select button.</p> <p>Note Clicking the Select button opens the Select PE Device window. (See the “Selecting a PE Device” section on page 11-23).</p> <p>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.</p> <p>The Device Name specified must match that of a PE device with role type of N-PE.</p>

Table 11-3 *Field Descriptions for the L3VPN - CE to CE Diagnostics - Test Setup Window (continued)*

Field	Valid for Test Type	Description
LSP Endpoint Loopback IP Address	L3VPN - PE to PE Core only	<p>Enter the BGP next hop if different from the BGP router ID of the peer PE. You can enter the loopback IP address, or you can enter the loopback name that will be resolved to the IP address.</p> <p>When testing the core, an MPLS OAM ping and trace is performed from the local PE to the remote PE. The destination of this ping causes an LSP to be selected based on the routing information on the local PE.</p> <p>Customer traffic uses the BGP next hop address of the customer route as its destination, and to select the LSP. Make sure that the IP prefix Diagnostics tests to matches the BGP next hop address used by the customer traffic. This ensures that Diagnostics tests the same LSP as the customer traffic traverses.</p> <p>In the case of L3VPN - PE to PE core testing, Diagnostics does not have any customer route information. Diagnostics therefore has no way to determine the BGP next hop and chooses the ping destination, not based on the next hop, but on the BGP router ID on the remote PE.</p> <p>In some network configurations, this router ID does not match the next hop used by the customer traffic and the incorrect (or no) LSP is tested.</p> <p>This happens when:</p> <ul style="list-style-type: none"> • The BGP router ID is the address of a loopback that has no LSP assigned to it. • The BGP router ID is not the address of a loopback. • The customer has several LSPs defined and the customer traffic is using a different LSP than the router ID gives. • The customer has several LSPs defined and the customer traffic switches LSP based on a routemap. <p>In the above bullet points you need to provide the correct BGP next hop.</p> <p>Note By specifying the LSP Endpoint Loopback IP Address, Diagnostics has the capability to test and detect core failures on multiple LSPs in the MPLS core.</p> <p>See the “Configuring the LSP Endpoint Loopback IP Address for a MPLS - PE to PE Test” section on page 11-34 for further information.</p>
PE Access CircuitInterface	L3VPN - CE to CE L3VPN - PE to attached CE L3VPN - CE to PE across Core L3VPN - PE to PE in VRF	<p>Enter the interface name of the PE Access Circuit Interface in the PE Access Circuit Interface field or select the PE Access Circuit Interface by clicking the Select button.</p> <p>Note Clicking the Select button opens the Select Device Interface window (see the “Selecting a PE Access Circuit Interface” section on page 11-24).</p> <p>You must specify a valid 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 Prime Provisioning device inventory.</p>

Table 11-3 **Field Descriptions for the L3VPN - CE to CE Diagnostics - Test Setup Window (continued)**

Field	Valid for Test Type	Description
CE Access Circuit Interface IP Address	L3VPN - CE to CE	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.
	L3VPN PE to attached CE	When a PE Access Circuit Interface configured using IPv4 addressing and with a /30 subnet mask (255.255.255.252) or a /31 subnet mask (255.255.255.254) is selected, the CE Access Circuit Interface IP Address field is auto-completed with the remaining host address from that /30 or /31 subnet. When a PE Access Circuit Interface configured with a /31 mask (255.255.255.254) subnet mask has been manually entered, an attempt to derive the CE access circuit interface IP address is only made after the test is initiated. In this instance, the CE Access Circuit Interface IP Address field is not auto-completed before the OK button is clicked.
	L3VPN - CE to PE across Core	It is not possible to derive the correct CE access circuit interface IP address in cases where the PE access circuit interface is using IP unnumbered or the CE access circuit interface is on a different subnet. The test supports managed and unmanaged Cisco CE devices, and non-Cisco CE devices.
Pings Ignored	L3VPN - CE to CE	Check this check box to specify that there is an ACL configured on the CE that will ignore ping and trace route packets originating from the provider core network.
	L3VPN - PE to attached CE	
	L3VPN - CE to PE across Core	
Customer Device IP Address	L3VPN - CE to CE	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.
	L3VPN - PE to attached CE	
	L3VPN - CE to PE across Core	
Find by Service	All	Click the Find by Service button to open the Populate using VPN/VRF window. The Populate using VPN/VRF window allows you to configure the test using customer VPN/VRF information (see the “Configuring Using Customer VPN/VRF Information” section on page 11-29.)
OK button	All	Click OK to run the test.
Clear button	All	Click Clear to reset all the fields in the window.

Step 4 Click **OK** to run your test after all the required fields are completed.

The Progress window appears. See the [“Progress Window” section on page 11-37.](#)

Selecting a PE Device

Click the **Select** button (for the Local/Remote PE Device Name) to open the Select PE Device window (see [Figure 11-11](#)) 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.

**Note**

You can configure the default value of the Diagnostics device selector, as shown in [Figure 11-11](#). Possible values are Device Name, Provider, and PE Region Name.

Figure 11-11 Select PE Device Window

#	Device Name	Provider	PE Region Name
1	iscind-crs-1	Provider456	Providerregion
2	iscind-7609-1	Provider456	Providerregion

**Note**

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 Prime Provisioning inventory, this overrides anything entered in the Local/Remote PE Device Name field (see [Figure 11-9](#).) This search feature is useful in large networks, where you have a large number of PEs.

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 11-12](#)) 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.

Figure 11-12 Select Device Interface Window

#	Interface Name	IPV4/IPV6 Address	VRF Name	Interface Description
1	ATM0/3/0/0			
2	ATM0/3/0/1			
3	ATM0/3/0/2			
4	ATM0/3/0/3			
5	GigabitEthernet0/1/0/0	19.67.11.5/31		Link to ABR1(12410-sdr-3)
6	GigabitEthernet0/1/0/1	19.67.11.7/31		L2VPN Link to cl-12810-1
7	GigabitEthernet0/1/0/2			L2VPN CE Link to MLS-1 (cl-7201-2)
8	GigabitEthernet0/1/0/2.15	15.1.2.2/31	ioxgreen	VRF GREEN Link to MLS-1(CE3)
9	GigabitEthernet0/1/0/2.15	2001:db80:aace:1::1/64	ioxgreen	VRF GREEN Link to MLS-1(CE3)
10	GigabitEthernet0/1/0/2.18	18.1.2.2/31	ioxwhite	

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 Prime Provisioning inventory, this overrides anything entered in the Local/Remote PE Access Circuit Interface field (see [Figure 11-9](#)).

[Table 11-4](#) provides field descriptions for the Select Device Interface window.

**Timesaver**

Enter an appropriate search pattern first using the Show Device Interfaces with the drop-down box and the matching field (see [Figure 11-12](#)). This saves large, time-consuming, and unnecessary searches which could occur in large networks. [Table 11-4](#) provides field descriptions for the Select Device Interface window.

Table 11-4 *Field Descriptions for the Select Device Interface Window*

Field	Description
Show Device Interfaces with	The Show Devices with drop-down box allows you to refine your search results. Select Interface Name, IPV4 Address, IPV6 Address, VRF Name or Interface Description from the drop-down menu to select the category to further refine the results of your search.
matching (optional field)	Enter information into the matching field to refine your search further within the category you selected in the Show Devices with drop-down box. You can enter text as a partial string; wildcards are also supported.
LDP Termination Only	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.
Find	Click Find to run your search using the information you configured in the Select Device Interface window.
Interface Name	Displays the list of interfaces found after you have run your search. Click on the Interface Name column heading to sort your list of interface names.
IPV4/IPV6 Address	Displays the list of IPV4/IPV6 addresses found after you have run your search. Click on the IPV4/IPV6 Address column heading to sort your list of IPV4/IPV6 addresses. You can choose the IPV6 address either by selecting it from the existing list or by manually entering it.
VRF Name	Displays the list of VRF names found after you have run your search. Click on the VRF Name column heading to sort your list of VRF names.
Interface Description	Displays the list of interface descriptions found after you have run your search. Click on the Interface Description column heading to sort your list of interface descriptions.
Row per page	Displays the row number of the rows displayed in the table. Click the corresponding radio button to select a row in the table.
Select	Click Select to confirm your selection in the table. The L3VPN - CE to CE Diagnostics - Test Setup Window appears with the PE Access Circuit Interface fields populated with the values you selected in the table.
Cancel	Click Cancel to close the Select Device for VRF Search window.

**Tip**

We recommend using the Interface Description to describe customer connection details. Diagnostics allows you to search on the Interface Description, for example, on a customer circuit ID. See the [“Selecting, Configuring, and Running a L3VPN - CE to PE Across Core Test”](#) section on page 11-31, and the [“Selecting, Configuring, and Running a L3VPN - PE to PE Test”](#) section on page 11-32 for information.

Testing Across Cisco IOS Multilink Access Circuit Interfaces

Diagnostics supports troubleshooting across Cisco IOS multilink access circuit interfaces. Troubleshooting is performed on the multilink bundle interface only. No troubleshooting of the individual bundle links or multilink specific troubleshooting is performed. The following multilink technologies are supported:

- Multilink PPP over Frame Relay (Multilink group interface configuration)
- Multilink PPP over Frame Relay (Virtual-Template interface configuration)
- Multilink PPP over ATM (Multilink group interface configuration)
- Multilink PPP over ATM (Virtual-Template interface configuration)
- Multilink PPP over Serial
- Multilink Frame Relay

**Note**

Multilink is supported in Cisco IOS only and not Cisco IOS XR.

**Note**

No Layer 2 Frame Relay, ATM, or Ethernet troubleshooting is performed for multilink access circuit interfaces.

Each multilink bundle has a number of interfaces associated with it. When configuring an MPLS VPN Connectivity Verification test over a multilink access circuit, you must ensure you enter the correct interface in the PE Access Circuit Interface field of the MPLS VPN Test Configuration window. The interface which you must enter varies depending on the multilink configuration used. [Table 11-5](#) details the interface that must be entered in the PE Access Circuit Interface field for each multilink technology.

Table 11-5 Multilink Interfaces

Multilink Technology	PE Access Circuit Interface
ML-PPPoFR (Multilink Group)	Multilink interface representing the multilink bundle.
ML-PPPoFR (Virtual-Template)	Virtual-Access interface representing the multilink bundle.
ML-PPPoATM (Multilink Group)	Multilink interface representing the multilink bundle.
ML-PPPoATM (Virtual-Template)	Virtual-Access interface representing the multilink bundle.
ML-PPPoSerial	Multilink interface representing the multilink bundle.
ML-FR	Frame Relay interface on which the Virtual Circuit is configured. This might be the Multilink Frame Relay (MFR) interface or a Frame Relay subinterface on the MFR interface.

With the exception of Multilink Frame Relay (MFR), the interface that represents the multilink bundle must be entered in the PE Access Circuit Interface field. For Multilink Frame Relay, the Frame Relay interface, or subinterface against which the Virtual Circuit is configured must be entered. This might be the MFR interface or a subinterface of the MFR interface. In all cases the interface entered in the PE Access Circuit Interface field should have an IP address and VRF and be in the up/up state.

To determine the valid multilink bundle interfaces on a PE device, use the **show ppp multilink** or **show frame-relay multilink** IOS command. If there are no active multilink bundles on your PE device, then there might be none configured or all bundle links for any configured multilink bundles might be in the down/down state.

**Note**

Virtual-Access interfaces are dynamically created and assigned. The multilink bundle to which a Virtual Access interface belongs and the role it plays can change as interface states change. As a result Virtual Access interfaces are not stored in the Prime Provisioning/Diagnostics repository. When configuring a VPN Connectivity Verification Test using a Virtual Access interface, you must manually enter the interface name into the PE Access Circuit Interface field of the MPLS VPN Test Configuration window. It is not possible to select Virtual Access interfaces from the Interface Selection popup dialog box.

Configuring Using Customer VRF Information

You need to supply PE hostname or PE interface details when entering information into the MPLS VPN Connectivity Verification window. In certain instances, you might not know the PE hostname or PE interface details. However, this information can be identified through a corresponding and known VRF name. You can identify a corresponding VRF name using a VRF search.

**Note**

To successfully find an interface by VRF Name, you must have previously run the Prime Provisioning Task Manager Collect Configuration task to upload the VRF names into Prime Provisioning. The VRF search is based on the information within the latest Collect Configuration task run. For details of how to perform a Task Manager Collect Configuration task, see [Device Configuration Collection, page 11-11](#).

- Step 1** Click the **Find by VRF** button in the MPLS VPN Connectivity Verification window.
The Select Device for VRF Search window appears.

**Note**

The fields displayed in the Select Device for VRF Search window are initially empty, regardless of whether any PE data fields have been populated or not.

- Step 2** Configure the fields displayed in the Select Device for VRF Search window.
[Table 11-6](#) provides field descriptions for the Select Device for VRF Search window.

**Timesaver**

Enter an appropriate search pattern first. This saves large, time-consuming, and unnecessary searches which could occur in large networks. Enter a VRF name pattern and click the Find button. For example, entering *t** and clicking Find provides a list of all VRFs starting with the letter *t*. You can further filter your list of results by selecting from the Show Devices with drop-down box, entering information into the matching field, and clicking Find. [Table 11-6](#) provides field descriptions for the Select Device for VRF Search window.

Table 11-6 *Field Descriptions for the Select Device for VRF Search Window*

Field	Description
VRF Search String	Enter a VRF name string to search on. You can enter the VRF name string as a partial string; wildcards are also supported.
Show Devices with	The Show Devices with drop-down box allows you to refine your search results. Select Device Name, Interface Name, IPV4 Address, IPV6 Address or Interface Description from the drop-down menu to select the category to further refine the results of your search.
matching (optional field)	Enter information into the matching field to refine your search further within the category you selected in the Show Devices with drop-down box. You can enter text as a partial string; wildcards are also supported.
Find	Click Find to run your VRF search using the information you configured in the Select Device for VRF Search window.
Device Name	Displays the list of device names found after you have run your search. Click on the Device Name column heading to sort your list of device names.
Interface Name	Displays the list of interfaces found after you have run your search. Click on the Interface Name column heading to sort your list of interface names.
IPV4/IPV6 Address	Displays the list of IPV4/IPV6 addresses found after you have run your search. Click on the IPV4/IPV6 Address column heading to sort your list of IPV4/IPV6 addresses. You can choose the IPV6 address either by selecting it from the existing list or by manually entering it.
VRF Name	Displays the list of VRF names found after you have run your search. Click on the VRF Name column heading to sort your list of VRF names.
Interface Description	Displays the list of interface descriptions found after you have run your search. Click on the Interface Description column heading to sort your list of interface descriptions.
Rows per page	Displays the row number of the rows displayed in the table. Click the corresponding radio button to select a row in the table.
Select	Click Select to confirm your selection in the table. The L3VPN - CE to CE Diagnostics - Test Setup window appears with the PE Device Name and PE Access Circuit Interface fields populated with the values you selected in the table.
Cancel	Click Cancel to close the Select Device for VRF Search window.

Step 3 Click **Find** to start your search.

The table displayed in the Select Device for VRF Search window is populated with your search results.



Tip Click on the column headings to sort the information displayed in each column.

**Tip**

The table automatically widens when required to display the information displayed in the VRF Name and Interface Description columns. When the table widens, use the horizontal scrollbar to scroll to the right side of the window.

Step 4 (Optional) Refine your search results by configuring the Show Devices with drop-down box and the matching field.

Click **Find** to refresh the table with the results of your search.

Step 5 Click the radio button to select the PE Device Name and corresponding Interface Name you require.

Step 6 Click **Select**.

The Select Device for VRF Search window closes. The L3VPN - CE to CE Diagnostics - Test Setup window appears with the PE Device Name and PE Access Circuit Interface fields populated with the values you selected.

Configuring Using Customer VPN/VRF Information

Diagnostics can be used standalone, without any dependency on other Prime Provisioning functionality. However, if Prime Provisioning VPN/VRF Provisioning functionality is used to provision VPN/VRFs within the network, this provisioning information, associated with the customer and VPN/VRF, 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/VRF, 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/VRF information is only available if the Prime Provisioning VPN/VRF Provisioning functionality is used to provision VPN/VRFs within the network.

Step 1 Click the **Find by Service** button in the L3VPN - CE to CE Diagnostics - Test Setup window.

The Populate using VPN/VRF window appears.

Step 2 Configure the fields displayed in the Populate using VPN/VRF window.

[Table 11-7](#) provides field descriptions for the Populate using VPN/VRF window.

Table 11-7 Field Descriptions for the Populate using VPN/VRF Window

Field	Description
Customer Details	
Customer Name	Click the Select button to select a customer from the Select Customer pop-up window.
VPN/VRF Name	Click the Select button to select a VPN/VRF name from the VPN/VRF name pop-up window.
	Note You must select a Customer Name before you can select a VPN/VRF Name.
Site Details	

Table 11-7 *Field Descriptions for the Populate using VPN/VRF Window (continued)*

Field	Description
Local Site	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/VRF Name before you can select a local site.
Remote Site	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/VRF Name before you can select a remote site. Note The Remote Site field is not available for the PE to attached CE test type.

Step 3 Click **OK**.

The L3VPN - CE to CE Diagnostics - Test Setup window reappears. The required fields are populated based on the customer VPN/VRF information you provided in the Populate using VPN/VRF 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 L3VPN - CE to CE Diagnostics - Test Setup window that have been automatically populated.

Step 4 Click **OK** on the L3VPN - CE to CE Diagnostics - Test Setup window to run the test.

The Progress window appears (see the [“Progress Window”](#) section on page 11-37).

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. See [VPN Topologies, page 11-49](#) for details of the configuration required and how the test results should be interpreted for each supported VPN topology.

Selecting, Configuring, and Running a L3VPN - PE to Attached CE Test

This section details how to select, configure, and run a L3VPN - PE to attached CE test type.

Step 1 From the Diagnostics menu, select the L3VPN - PE to Attached CE test type.

Step 2 Click on the L3VPN - PE to attached CE connectivity verification test type.

See the “[L3VPN - PE to Attached CE Connectivity Test](#)” section on page 11-15 for information on the PE to attached CE connectivity verification test type.

The MPLS VPN Connectivity Verification Configuration window appears ([Figure 11-13](#)) displaying the fields corresponding to the PE to attached CE test type. The MPLS VPN Connectivity Verification Configuration window allows you to configure the connectivity test you would like to perform.

Figure 11-13 L3VPN - PE to Attached CE Test Type

Test Representation

Local Site Remote Site

Customer Device CE PE MPLS Core PE CE Customer Device

Local Site Find by VRF

PE Device Name*: Select

PE Access Circuit Interface*: Select

CE Access Circuit Interface IP Address*: ☐ Pings Ignored

Customer Device IP Address:

Find by Service Clear Run

Note: * - Required Field

Note: *1 - Optional - If the Access Circuit is a /30 or /31 subnet [only for IPv4]

Note: * - To launch troubleshooting on 6VPE

- Select or specify PE Access Circuit Interface with IPv6 address
- Specify a Global Unicast IPv6 address for the CE Access Circuit Interface IP Address
- Optional - Specify a Global Unicast IPv6 Address for the Customer Device IP Address

The L3VPN - PE to Attached CE window displays the following components:

- Network diagram
- Local Site configuration area

These components and the test scope are described in further detail in the “[Selecting, Configuring, and Running a L3VPN - CE to CE Test](#)” section on page 11-19.

Step 3 Configure the fields in the L3VPN - PE to Attached CE window as required.

[Table 11-3 on page 11-21](#) provides descriptions of the fields applicable to the L3VPN - PE to attached CE test type.

Step 4 Click **OK** to run your test after all the required fields are completed. The Progress window appears. See the “[Progress Window](#)” section on page 11-37.

Selecting, Configuring, and Running a L3VPN - CE to PE Across Core Test

This section details how to select, configure, and run a L3VPN - CE to PE across core test type.

Step 1 From the Diagnostics menu, select the L3VPN - CE to PE across Core test type.

Step 2 Click on the L3VPN - CE to PE across Core connectivity verification test type.

See the “[L3VPN - CE to PE Across Core Connectivity Test](#)” section on page 11-16 for information on the L3VPN - CE to PE across core connectivity verification test type.

The L3VPN - CE to PE Across MPLS Core Diagnostics - Test Setup window appears (Figure 11-14) displaying the fields corresponding to the L3VPN - CE to PE across core test type. The L3VPN - CE to PE Across MPLS Core Diagnostics - Test Setup window allows you to configure the connectivity test you would like to perform.

Figure 11-14 L3VPN - CE to PE Across Core Test Type

L3VPN - CE to PE across Core

Test Representation

Local Site: Customer Device, CE, PE, MPLS Core, PE, CE, Remote Site: Customer Device

Local Site Find by VRF

PE Device Name *: Select

PE Access Circuit Interface *: Select

CE Access Circuit Interface IP Address *1: ☐ Pings Ignored

Customer Device IP Address:

Remote Site Find by VRF

PE Device Name *: Select

PE Access Circuit Interface *: Select

Find by Service Clear Run

Note: * - Required Field
 Note: *1 - Optional - if the Access Circuit is a /30 or /31 subnet [only for IPv4]
 Note: * - To launch troubleshooting on 6VPE
 - Select or specify PE Access Circuit Interface with IPv6 address
 - Specify a Global Unicast IPv6 address for the CE Access Circuit Interface IP Address
 - Optional - Specify a Global Unicast IPv6 Address for the Customer Device IP Address

The L3VPN - CE to PE Across Core window displays the following components:

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

These components and the test scope are described in further detail in the [“Selecting, Configuring, and Running a L3VPN - CE to CE Test”](#) section on page 11-19.

Step 3 Configure the fields in the L3VPN - CE to PE Across Core window as required.

[Table 11-3 on page 11-21](#) provides descriptions of the fields applicable to the L3VPN - CE to PE across core test type.

Step 4 Click **OK** to run your test after all the required fields are completed.

The Progress window appears. See the [“Progress Window”](#) section on page 11-37.

Selecting, Configuring, and Running a L3VPN - PE to PE Test

This section details how to select, configure, and run a L3VPN - PE to PE test type.

Step 1 From the Diagnostics menu, select the L3VPN - PE to PE test type.

See the “[L3VPN - PE to PE in VRF Connectivity Test](#)” section on page 11-16 for information on the L3VPN- PE to PE (in VRF) connectivity verification test type.

The L3VPN- PE to PE in VRF Diagnostics - Test Setup window appears ([Figure 11-15](#)) displaying the fields corresponding to the L3VPN - PE to PE in VRF test type. The L3VPN- PE to PE in VRF Diagnostics - Test Setup window allows you to configure the connectivity test you would like to perform.

Figure 11-15 L3VPN - PE to PE Test Type

3VPN - PE to PE in VRF

Test Representation

Local Site

Customer Device

CE

PE

MPLS Core

PE

CE

Remote Site

Customer Device

Local Site Find by VRF

PE Device Name * : Select

PE Access Circuit Interface * : Select

Remote Site Find by VRF

PE Device Name * : Select

PE Access Circuit Interface * : Select

Find by Service Clear Run

Note: * - Required Field
Note * - To launch troubleshooting on 6VPE, select interfaces with IPv6 address

The L3VPN - PE to PE in VRF Diagnostics - Test Setup window displays the following components:

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

These components and the test scope are described in further detail in the “[Selecting, Configuring, and Running a L3VPN - CE to CE Test](#)” section on page 11-19.

Step 2 Configure the fields in the L3VPN - PE to PE in VRF Diagnostics - Test Setup window as required.

[Table 11-3 on page 11-21](#) provides descriptions of the fields applicable to the L3VPN - PE to PE in VRF test type.

Step 3 Click **OK** to run your test after all the required fields are completed.

The Progress window appears. See the “[Progress Window](#)” section on page 11-37.

Selecting, Configuring, and Running a MPLS - PE to PE Test

This section details how to select, configure, and run a L3VPN - PE to PE (Core) test type.

Step 1 From the Diagnostics menu, select the MPLS - PE to PE test type.

Step 2 Click on the MPLS - PE to PE connectivity verification test type.

See the “[L3VPN - PE to PE Connectivity Test](#)” section on page 11-17 for information on the PE to PE connectivity verification test type.

The MPLS - PE to PE window appears ([Figure 11-16](#)) displaying the fields corresponding to the MPLS - PE to PE test type. The MPLS - PE to PE window allows you to configure the connectivity test you would like to perform.

Figure 11-16 MPLS - PE to PE Test Type

MPLS - PE to PE

Test Representation

Local Site: Customer Device, CE, PE. Remote Site: CE, PE, Customer Device. MPLS Core connects the two PE devices.

Local Site Find by VRF

PE Device Name*: Select

LSP Endpoint Loopback Interface*1:

Remote Site Find by VRF

PE Device Name*: Select

LSP Endpoint Loopback Interface*1:

Find by Service Clear Run

Note: * - Required Field
 Note: *1 - Optional - In networks where there are multiple LSPs between the specified PEs, it is recommended that at least the Remote Site LSP endpoint is specified. By default the BGP router-id will be used.

The MPLS - PE to PE window displays the following components:

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

These components and the test scope are described in further detail in the “[Selecting, Configuring, and Running a L3VPN - CE to CE Test](#)” section on page 11-19.

Step 3 Configure the fields in the MPLS - PE to PE window as required.

[Table 11-3 on page 11-21](#) provides descriptions of the fields applicable to the L3VPN - PE to PE test type.

Step 4 Click **OK** to run your test after all the required fields are completed.

The Progress window appears. See the “[Progress Window](#)” section on page 11-37.

Configuring the LSP Endpoint Loopback IP Address for a MPLS - PE to PE Test

This section details how to configure the LSP endpoint loopback interface and IP address for the MPLS - PE to PE test type.

Remote LSP Endpoint Loopback IP Address

L3 VPN Customer traffic uses the BGP next hop address of the customer route to select the LSP. When testing the core, an MPLS OAM ping and trace is performed from the local PE to the remote PE. To ensure that Diagnostics tests the same LSP as your traffic traverses, the IP prefix Diagnostics tests to is the BGP next hop address of the customer route.

Diagnostics does not have customer route information for the PE to PE core test type. Diagnostics therefore has no way to determine the BGP next hop. By default, Diagnostics chooses the ping and trace destination, not based on the next hop, but on the BGP router ID on the remote PE. In some network configurations, such as those with multiple cores, or with multiple loopback addresses used for control and data plane traffic, this BGP router ID might not match the next hop used by the customer traffic and the incorrect (or no) LSP is tested.

Local LSP Endpoint Loopback IP Address

The MPLS - PE to PE test type allows you to perform the test in the reverse direction when running the test in the forward direction fails to find the problem. Configuring the local LSP endpoint loopback IP address ensures that the test selects the correct LSP when the test is run in the reverse direction.

When Should I Specify the LSP Endpoint Loopback IP Address?

Specify the LSP endpoint loopback IP address when:

- The BGP router ID is the address of a loopback that has no LSP assigned to it.
- The BGP router ID is not the address of a loopback.
- Several LSPs are defined and the traffic is using a different LSP than the router ID provides.
- Several LSPs are defined and the traffic switches LSP based on a routemap.

**Note**

You must provide the correct BGP next hop when specifying the remote LSP endpoint.

Figure 11-17 displays an example network topology that illustrates the LSP Endpoint Loopback IP Address field usage. This example network topology has three logical MPLS cores and some of the PE BGP router-ids are not associated with a loopback interface. In addition, two of the CEs are dual homed to different cores.

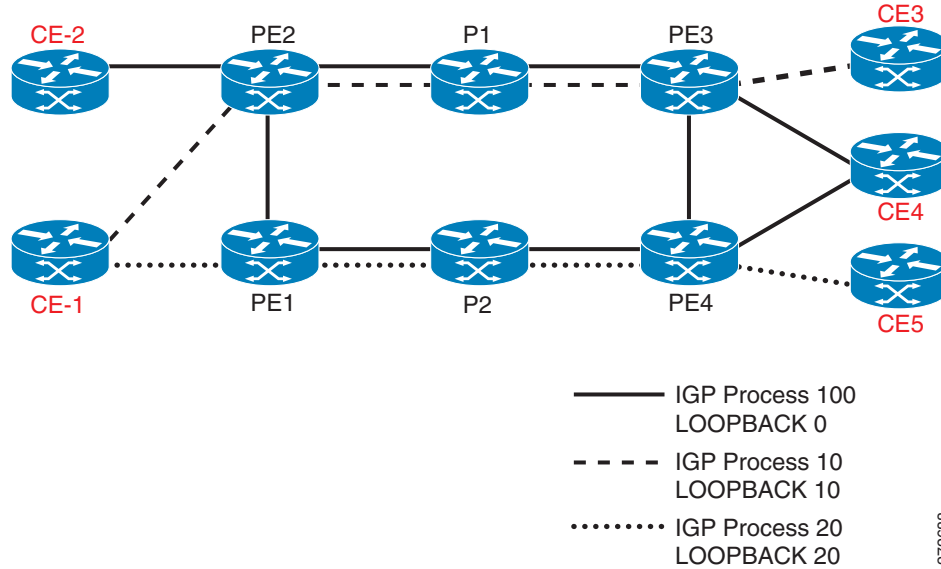
Figure 11-17 Example Network Topology

Table 11-8 provides IP addressing information relating to the example network topology displayed in Figure 11-17.

Table 11-8 IP Addressing

PE	BGP Router ID	Loopback 0	Loopback 10	Loopback 20
PE2	1.1.1.1	1.1.1.1	N/A	20.20.20.1
PE3	1.1.1.3	1.1.1.3	N/A	20.20.20.3
PE1	50.50.50.1	1.1.1.6	10. 10.10.1	N/A
PE4	50.50.50.3	1.1.1.8	10. 10. 10.3	N/A

Table 11-9 specifies the IP addresses that can be used as the remote LSP Endpoint IP Address to test each LSP.

Table 11-9 Inputs Required to Test Each LSP

LSP Under Test	For CE	Remote Site PE	Remote Endpoint
Solid line	CE-2	PE2	Not required as next hop is the BGP router-id.
Solid line	CE-4	PE4	1.1.1.8 (Loopback 0)
Solid line	CE-4	PE3	Not required as next hop is the BGP router-id.
Dotted line	CE-1	PE2	20.20.20.1 (Loopback 20)
Dotted line	CE-3	PE3	20.20.20.3 (Loopback 20)
Dashed line	CE-1	PE1	10. 10.10.1 (Loopback 10)
Dashed line	CE-5	PE4	10. 10.10.3 (Loopback 10)

Progress Window

The Progress window appears (see [Figure 11-18](#)) while the test is being performed.

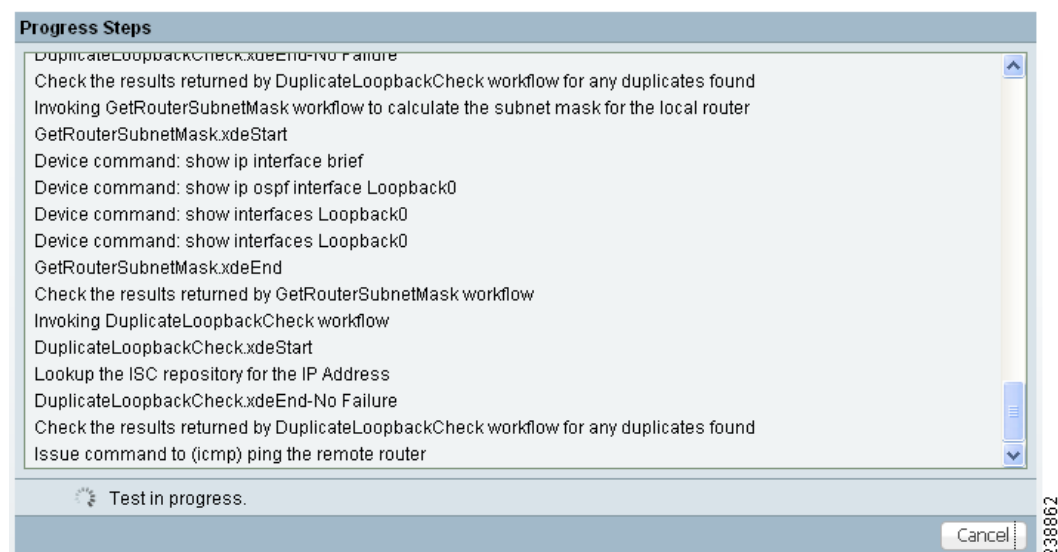


Note

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, the test type selected, whether a connectivity problem is identified, and the nature of this connectivity problem.

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

Figure 11-18 Progress Window



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 the [“Interpreting the Test Results” section on page 11-37](#), for further details.

Interpreting the Test Results

This section describes how to interpret your test results. This section contains the following information:

- [Data Path, page 11-39](#)
- [Test Details, page 11-41](#)
- [Test Log, page 11-42](#)
- [Export, page 11-43](#)

Upon completion of a MPLS VPN Connectivity Verification test, the Test Results window appears (see [Figure 11-19](#)).

Figure 11-19 Test Results Window with Failure Specific Additional Information Displayed

The screenshot displays the 'Test Results' window. At the top, a network diagram shows a path from CE (192.168.1.10) through PE (-/20) and P (20/17, 17/16, 16/No Label) to another CE (192.168.1.8). The path includes interfaces GigE1/0, GigE2/0, FE2/0, FE0/0, and FE4/0. Below the diagram, the 'Result' section shows a failure on router 'cl-test-core-7206-3'. The 'View' section has 'Test Details' selected. The 'Summary' states: 'LSP connectivity problem, control plane issue, from cl-test-core-12404-1 to cl-test-core-7206-3 for prefix 192.168.101.2/32.' The 'Possible Cause(s)' is 'CEF not enabled on router cl-test-core-7206-3.' The 'Recommended Action' is 'Enable CEF on router cl-test-core-7206-3.' The 'Device' is 'cl-test-core-12404-1' and the 'Command' is 'show interfaces POS3/3'. The output of the command is shown in a text area, indicating that POS3/3 is administratively down and line protocol is down. At the bottom right, there are buttons for 'Advanced', 'Re-test', and 'Cancel'. A vertical label '238864' is on the right side of the window.

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 11-10](#)).

The Test Results window consists of the following components:

Table 11-10 Field Descriptions for the Test Results Window

Field/Button	Description
Data path	See the “Data Path” section on page 11-39
Test Details	See the “Test Details” section on page 11-41
Test Log	See the “Test Log” section on page 11-42
Export button	The Export button appears when the Test Log radio button is selected. See the “Export” section on page 11-43.
Advanced button	Click the Advanced button to launch advanced troubleshooting. See the “Advanced Troubleshooting Options” section on page 11-43. The options available on this button are dynamically configured depending on the test result and the test type.

Table 11-10 Field Descriptions for the Test Results Window (continued)

Field/Button	Description
Re-test button	Click the Re-test button to rerun 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 the cancellation.

If multiple failures exist in the tested path, the failure reported is determined by the order in which Diagnostics performs troubleshooting. For the CE to CE connectivity test type, Diagnostics troubleshooting is performed in the following order:

1. Access circuit (local and remote).
2. MPLS Traffic Engineered (TE) tunnels.
3. MPLS core.
4. MPLS VPN edge.

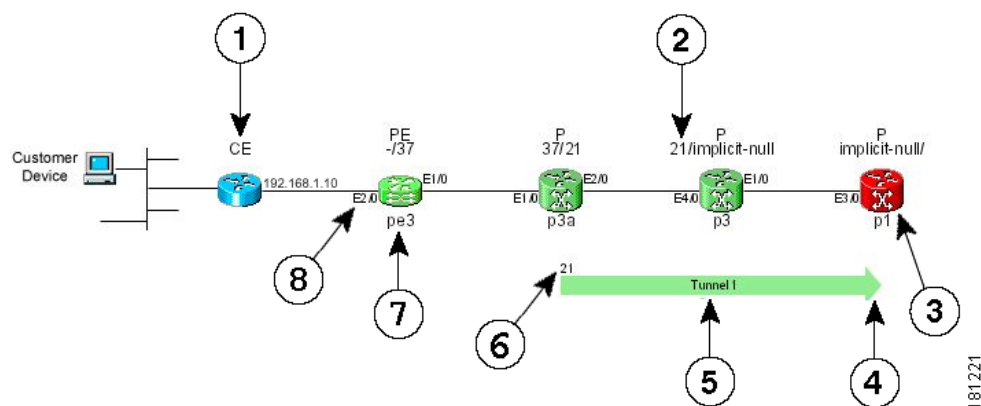
The other test types troubleshoot in the same order, but do not perform all of the steps.

**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 rerun.

Data Path

The Data Path (see [Figure 11-20](#)) shows a graphical representation of the path between the two sites that have been tested. If a failure is found on an MPLS Traffic Engineered tunnel, the tunnel is displayed in the Data Path. Any non-overlapping P-P, PE-P, or P-PE MPLS TE Tunnels found in the path before the point of failure will also be displayed in the datapath.

Figure 11-20 Data Path

1. Device Role (CE, PE, or P).
2. MPLS labels (ingress/egress).
3. Failed device.

4. Tunnel direction arrow.
5. Tunnel name.
6. Tunnel label.
7. Device hostname.
8. Interface name.

Where present, MPLS TE tunnels are displayed below the device path.






If a Customer Device IP address is specified, this IP address will appear beside the text “Customer Device.”

**Note**

An MPLS TE tunnel is displayed, only when it is found to be the cause of the connectivity failure.


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 11-11](#).

Table 11-11 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.
Yellow		Possible device failure.
Grey		Device access failure.

The link color used in the data path is described in [Table 11-12](#).

Table 11-12 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.

The following information is displayed for an MPLS Traffic Engineered tunnel:

- Tunnel name
- Tunnel direction (direction arrow)
- Tunnel label

**Note**

It is not possible to Telnet to a device from the Data Path in the Test Result window.

Test Details

The Test Details section of the Test Results window (see [Figure 11-19 on page 11-38](#)) displays a summary of the automated troubleshooting and diagnostics results, observations made during troubleshooting, additional failure-specific information, and recommended action. See [Failure Scenarios, page 11-57](#) for details of failures and observations reported by Diagnostics, and for a list of all IOS and IOS XR commands executed by Diagnostics as part of the troubleshooting.

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), Border Gateway Protocol (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 11-19 on page 11-38](#) shows an example Test Results window with failure specific information below the Test Details summary. The Test Details radio button is selected by default.

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 11-21](#) 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.

Figure 11-21 Test Results Window with Observation Notes

Test Representation

Result

View: ☒ Test Details ☐ Test Log

Summary: TE Tunnel connectivity problem.

Possible Cause(s): MPLS Traffic Engineering is not enabled globally on router tl-dev-12410-1-sdr-3. MPLS TE must be enabled globally on all routers involved in an MPLS Tunnel.

Recommended Action: Enable Traffic Engineering globally on router tl-dev-12410-1-sdr-3 by enabling *mpls traffic-eng* in configuration.

Note: A route map is configured on the PE tl-dev-12404-3 which may be causing route traffic to be lost

Note: A route map is configured on the PE tl-dev-crs1-1-sdr-1 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: tl-dev-12404-3	Router: tl-dev-crs1-1-sdr-1
Import map pass-all:	Import map pass-all:
<pre>route-policy pass-all pass end-policy </pre>	<pre>route-policy pass-all pass end-policy </pre>
Export map pass-all:	Export map pass-all:
<pre>route-policy pass-all pass end-policy </pre>	<pre>route-policy pass-all pass end-policy </pre>

Advanced Re-test Cancel

238865

Test Log

Click the Test Log (see [Figure 11-22](#)) radio button to display details of all troubleshooting and diagnostics steps in the order in which they were performed.

Figure 11-22 Test Results Window—Test Log

Test Representation

Result

View: ☒ Test Details ☐ Test Log

Summary: LSP connectivity problem from cl-test-edge-6509-1 to cl-test-ac-7200-10.

Possible Cause(s): Troubleshooting of the Layer 3 VPN has been unable to find the cause of the failure.

Recommended Action: Run the troubleshooting task again in the reverse direction using the Reverse Test option available on the Advanced button. You might also wish to perform route processor and line card consistency checks.

Note: The ICMP ping issued from PE cl-test-edge-6509-1 to 192.168.103.5 on PE cl-test-ac-7200-10 failed. The PE cl-test-edge-6509-1 has no IGP route to 192.168.103.5. Try troubleshooting IP connectivity between these devices.

Note: The mpls traceroute from cl-test-edge-6509-1 to 192.168.103.5 was not transmitted.

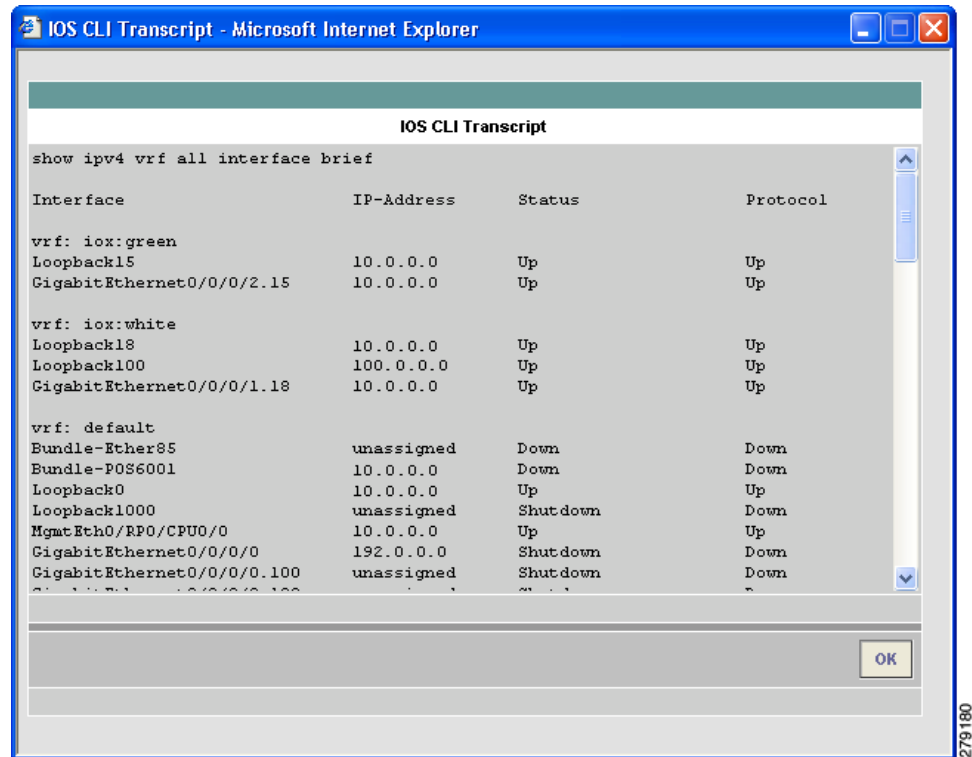
Warning: No LSP Endpoint Loopback IP Address was specified for the remote site host cl-test-ac-7200-10. The BGP router-id of the remote site host was used as the LSP endpoint for LSP troubleshooting. This may result in the incorrect LSP being tested.

Advanced Re-test Cancel

238863

Some steps require device interaction involving the execution of IOS or IOS XR CLI commands. These steps appear in the Test Log as hyperlinks. Clicking a hyperlink opens a pop-up window that displays the IOS or IOS XR CLI transcript for the step (see [Figure 11-23](#)). This transcript includes the IOS or IOS XR commands run and all resulting output.

Figure 11-23 IOS CLI Transcript Window



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 11-22 on page 11-42](#)). All steps displayed in the test log, including IOS and IOS XR 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.rtf*.

Step 2 Save the file.

Advanced Troubleshooting Options

This section describes advanced troubleshooting options, as follows:

- [Reverse Path Testing, page 11-44](#)

- [LSP Visualization, page 11-44](#)

Advanced troubleshooting provides further options that you can use to troubleshoot your network.

The advanced troubleshooting options supported are detailed in [Table 11-13](#).

Table 11-13 **Advanced Troubleshooting Options**

Advanced Troubleshooting Option	Description
Reverse path test	Available when a failure is found.
LSP Visualization	Available when no failure is found.
LSP Troubleshooting	Available when an IP failure is found.

The appropriate advanced troubleshooting options are made available through the Advanced drop-down button at the bottom of the Test Results window.

Reverse Path Testing



Note

The reverse path testing option is available for all test types except for the PE to attached CE test type.

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. In other cases, repeating the test in the reverse direction can result in a more precise diagnosis of the problem found. 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 misconfiguration on the downstream LSP neighbor. By repeating the test in the reverse direction, the misconfigured downstream router is encountered first and the LDP misconfiguration 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 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.

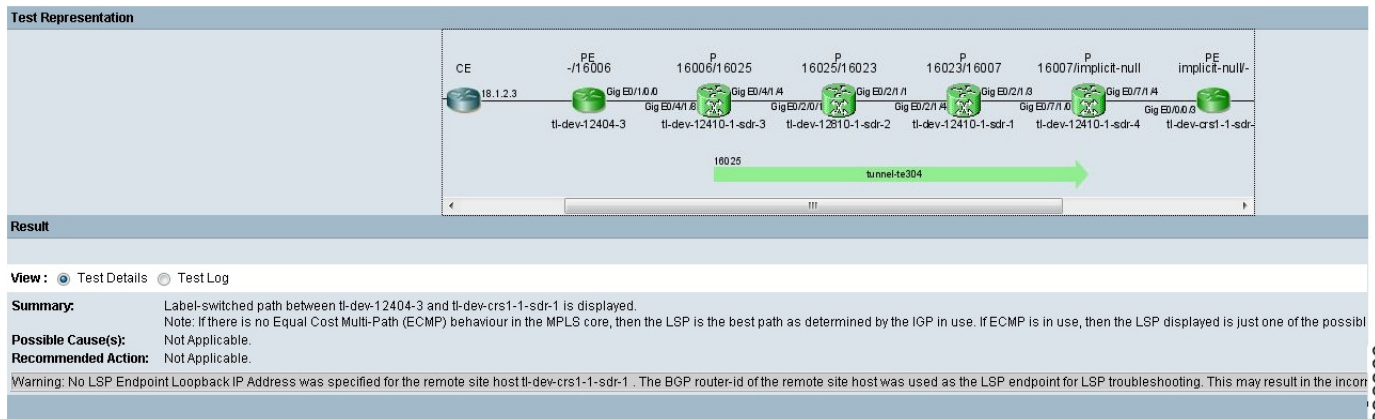
LSP Visualization



Note

LSP visualization is available for all test types except for the PE to attached CE test type.

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 11-24](#)). The LSP Visualization displays all intermediate non-overlapping PE to P, P to P and P to PE tunnels found in the forward path. The path shown is the path tested during the MPLS VPN Connectivity Verification test.

Figure 11-24 Test Results Window—LSP Visualization

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

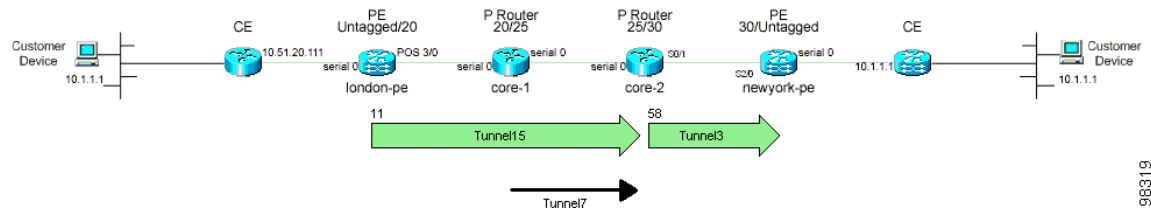
The Data Path displays the following for each PE to PE MPLS Traffic Engineered tunnel:

- Tunnel name
- Tunnel direction (direction arrow)
- Tunnel label
- Tunnel Type

**Note**

In cases where there are multiple MPLS TE Tunnels configured, the only tunnel that is displayed in the datapath will be the one that is actually carrying the traffic.

In the example below, Tunnel 7 is not displayed because it is overlapping, i.e. its headend is configured at the midpoint of Tunnel 15 which is configured on the upstream router.

Figure 11-25 Multiple MPLS TE Tunnel Configuration

For more details of what is displayed in the Data Path, see the [“Data Path” section on page 11-39](#).

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.

Switching Tunnel Checking Off—For Networks with Non-Cisco P Routers

During tunnel diagnostics, Diagnostics might be required to visit every device to determine if a tunnel is present at that point. Since Diagnostics does not log in to non-Cisco devices, this can result in a misdiagnosis of a fault occurring at the non-Cisco device (even though it might not be the actual source of the fault) as the troubleshooting workflow is unable to proceed. As a result, it is useful to disable tunnel diagnostics for networks that contain non-Cisco devices.

Tunnel diagnostics is enabled as default. The default value can be changed by an Admin user, within the the Prime Provisioning Control Center (**Administration tab > Control Center > Hosts**). Tunnel diagnostics can be enabled or disabled within the Command Flow Runner (cfr) component (parameter `disableTunnelDiagnostics`). When the appropriate `disableTunnelDiagnostics` parameter is set to true, Diagnostics does not perform tunnel diagnostics.

The Test Results window displays an observation message stating that Diagnostics tunnel diagnostics are disabled. The error message indicating a device is not in the inventory mentions that a possible cause is a non-Cisco device on the path, and that the error might be on this device or a near neighbor.

How Does Diagnostics Work?

This chapter describes how the Diagnostics application works.

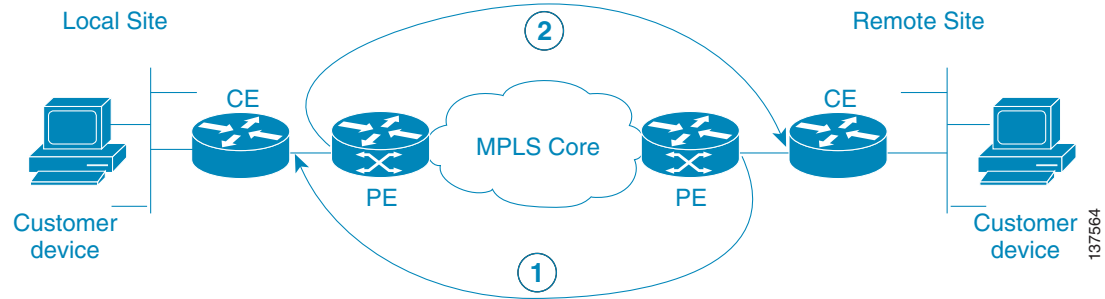
The MPLS VPN Connectivity Verification test consists of connectivity testing, troubleshooting, and diagnostics steps. The exact steps performed for each test depend upon the nature of the failure found and the location of the failure within the network. Due to the simple test configuration and result 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.

**Note**

The steps detailed in this chapter are illustrative of the types of tests that Diagnostics performs. However, this list of tests is not exhaustive; Diagnostics performs many more tests.

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 or to the CE 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, Prime Provisioning 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 11-26](#)).

Figure 11-26 IOS VRF Ping Connectivity Tests

1. The first stage (see Figure 11-26) 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.
2. The second stage (see Figure 11-26) 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.

Performing the connectivity test from the remote site PE to the local site CE first ensures that any problems with the local access circuit are found first. This means that any reverse-path MPLS VPN, MPLS core, and MPLS TE Tunnel problems will be found before forward-path problems.

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. Troubleshooting is performed in the following order:

1. Access circuit (local and remote).
 - a. L3 connectivity (VRF pings and trace to CE and Customer Device) and route checks.
 - b. L2 (ATM, Ethernet, Frame Relay, Serial) connectivity and status checks.
 - c. PE-CE routing protocol determination and status checks.
 - d. PE-CE routing protocol and MP-BGP redistribution checks.

2. MPLS VPN edge.
 - a. MP-BGP neighbor and VPN route checks.
 - b. VRF route limit and checks.
 - c. Route map presence checks.
 - d. PE-PE VRF (VRF pings and trace across MPLS core) connectivity checks.
 - e. PE MPLS OAM capability checks.
3. MPLS Traffic Engineered (TE) tunnels.
 - a. Tunnel connectivity (TE aware ping and trace) and status checks.
4. MPLS core.
 - a. IP connectivity (ICMP ping) checks.
 - b. LSP connectivity (LSP ping and trace) and status checks.
 - c. LSP datapath generation.
 - d. LSP fault localization.
 - e. LDP session and neighbor checks.
 - f. Label checks.
 - g. MPLS VPN edge.
 - h. VPN label checks.
 - i. VRF route target checks.

**Note**

Core troubleshooting will only be performed for PE devices which support the Cisco IOS MPLS LSP Ping and Traceroute feature. For details of supported device types and Cisco IOS versions with MPLS OAM support, see [Supported Hardware, IOS, and IOS XR Versions, page 11-3](#).

**Note**

Diagnostics troubleshoots the primary tunnel if it is configured with FRR protection and reports the possible failures found in the primary tunnel and backup tunnels (providing FRR protection to the primary tunnel). The backup tunnel troubleshooting is limited to tunnels that are configured to protect the FRR enabled primary tunnel configured between ABRs.

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.

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 five minutes. After five 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 Prime Provisioning server to the device. Ensure that the device login details configured in the Prime Provisioning 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 are 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.

VPN Topologies

This appendix details how to perform an MPLS VPN Connectivity Verification test for the supported VPN topologies. This appendix contains the following sections:

- [Testing with Full Mesh VPN Topology, page 11-49](#)
- [Testing with Hub and Spoke VPN Topology, page 11-50](#)
- [Testing with Intranet/Extranet VPN Topology, page 11-56](#)
- [Testing with Central Services VPN Topology, page 11-57](#)

Testing with Full Mesh VPN Topology

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. For details of how to configure an MPLS VPN Connectivity Verification test for a full mesh VPN topology, see [Performing an MPLS VPN Connectivity Verification Test, page 11-18](#).

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:

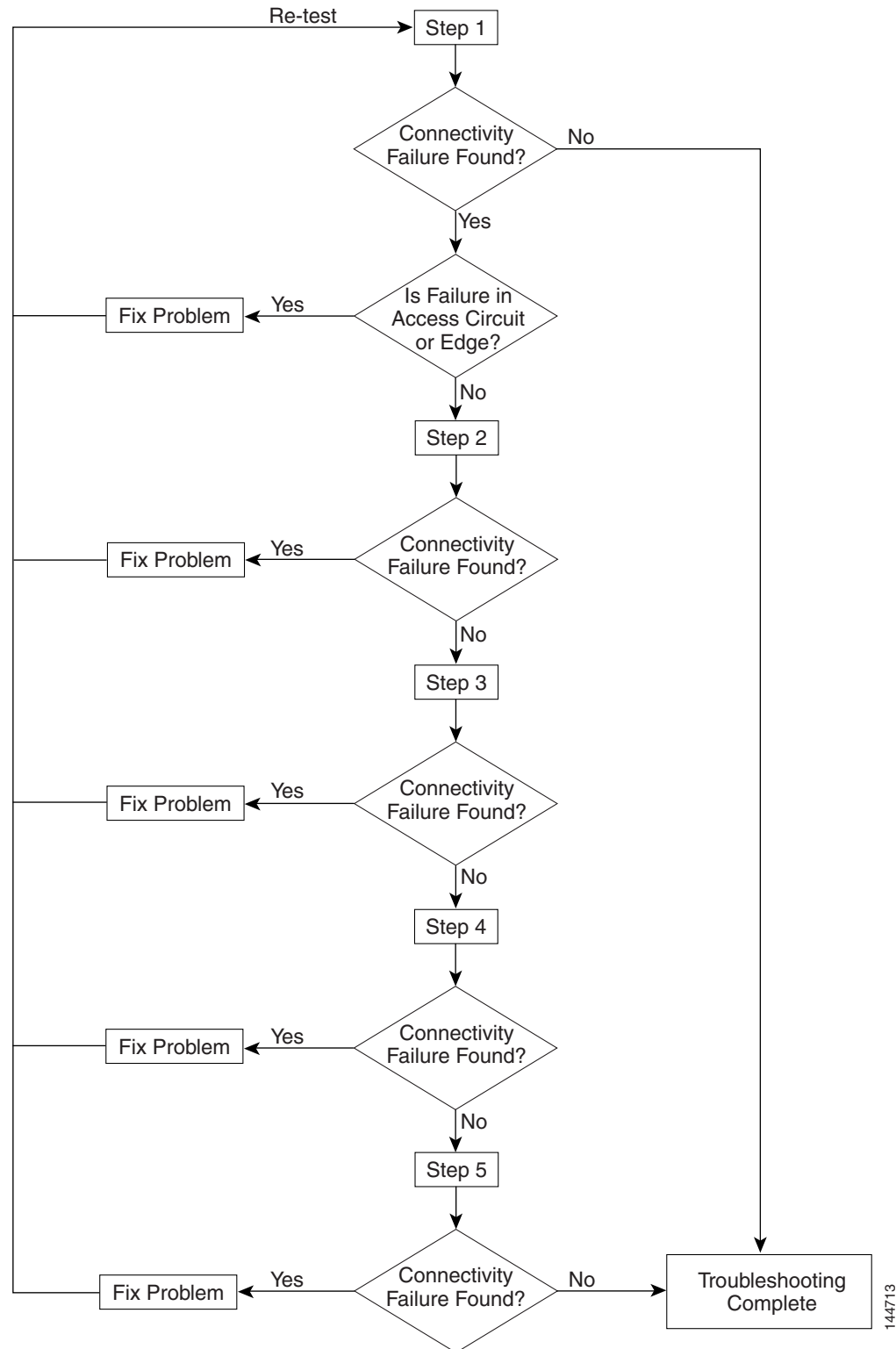
-
- Step 1** MPLS VPN Connectivity Verification test between the local and the remote sites.
 - Step 2** MPLS VPN Connectivity Verification test between the local site and the hub CE interface that is attached to the hub PE interface importing routes.
 - Step 3** MPLS VPN Connectivity Verification test 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.
-

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 11-27](#) shows the workflow for testing a hub and spoke VPN.

After fixing a problem reported in [Step 1](#) through [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](#) might be incorrect and should be ignored. [Step 2](#) through [Step 5](#) should be performed until the problem is diagnosed correctly.

Figure 11-27 Workflow

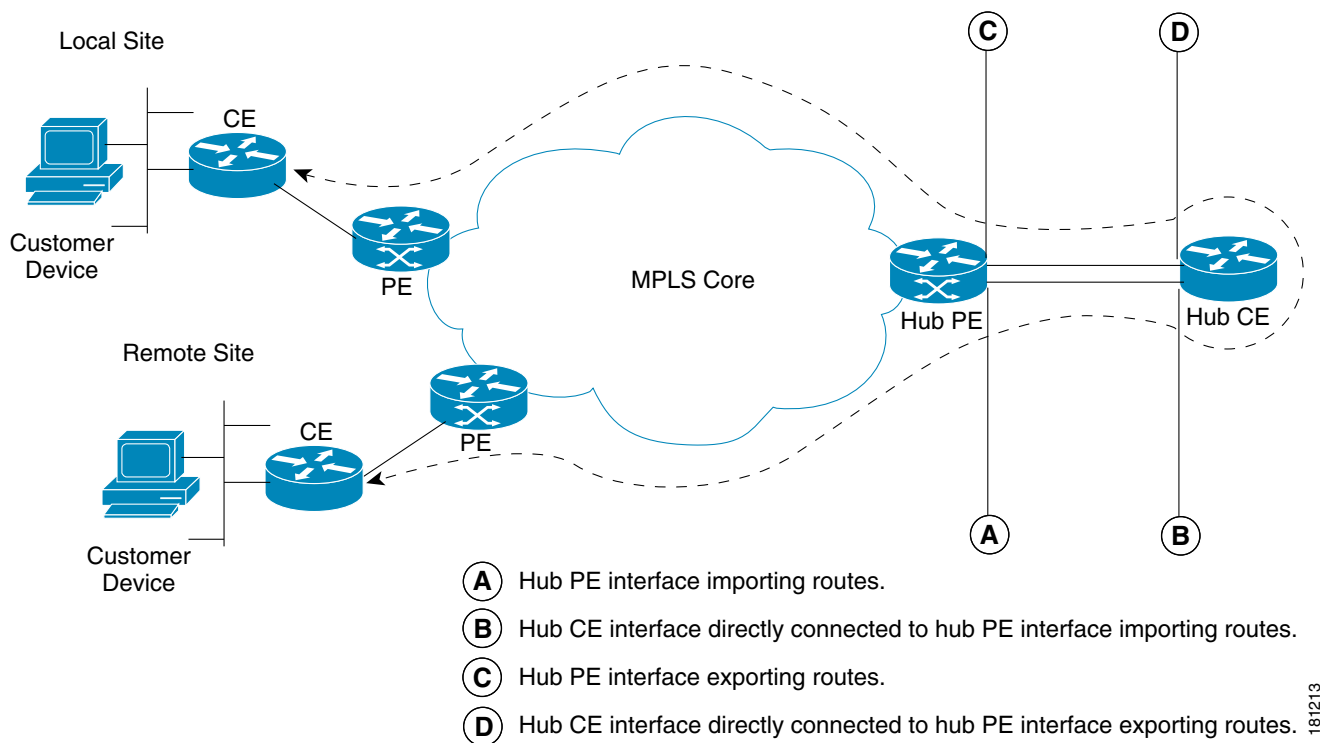
1. You should perform an MPLS VPN Connectivity Verification test between the local and remote sites. If this test finds no connectivity problems, then no further troubleshooting is required. If this test reports a connectivity failure caused by an MPLS problem, you should ignore the test result and move to 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 in the core, the MPLS VPN Connectivity Verification test performed in 1. might 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.

Figure 11-28 illustrates the MPLS VPN Connectivity Verification tests required to test connectivity between two sites in a hub and spoke VPN.

Figure 11-28 Testing a Hub and Spoke VPN Topology—Step 1

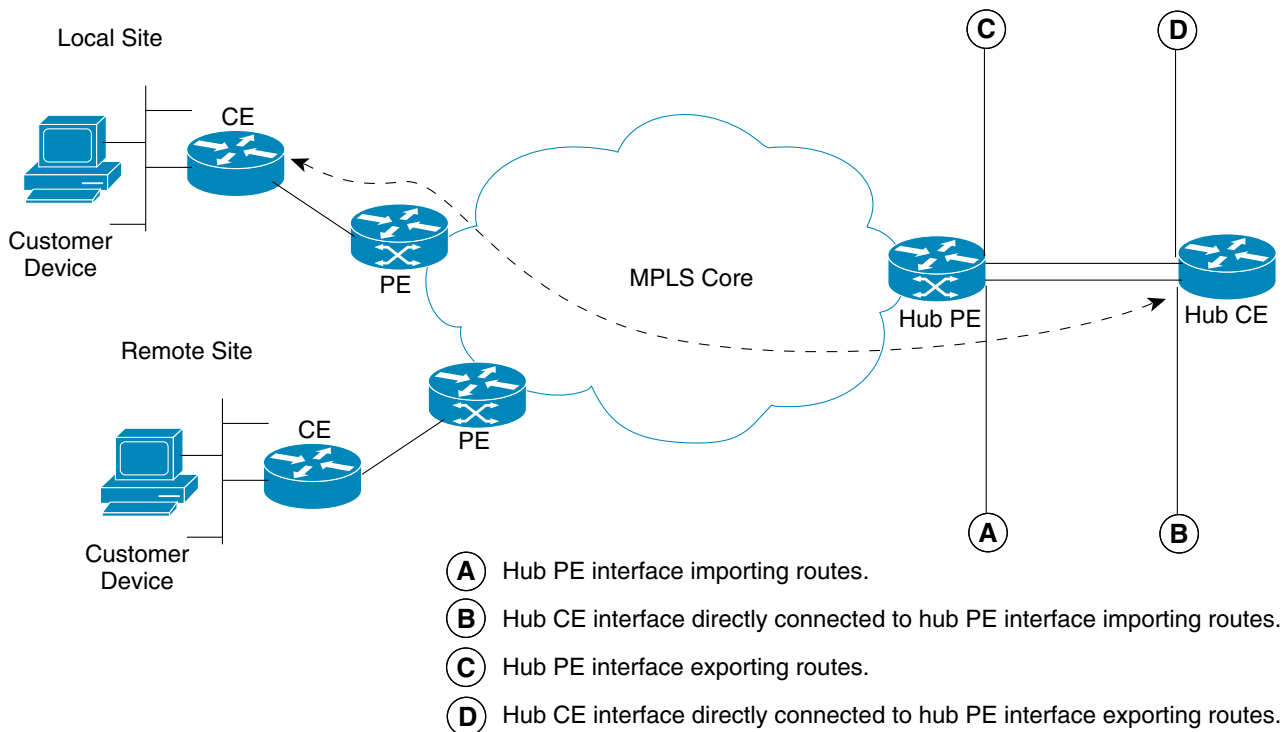


2. You should perform an MPLS VPN Connectivity Verification test between the local site (Spoke) and the hub CE interface that is attached to the hub PE interface which imports routes (shown in Figure 11-29 as B). When configuring the MPLS VPN Connectivity Verification test, the Local Site fields on the 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 interfaces that import routes (shown in Figure 11-29 as A and B), as shown in Table 11-14.

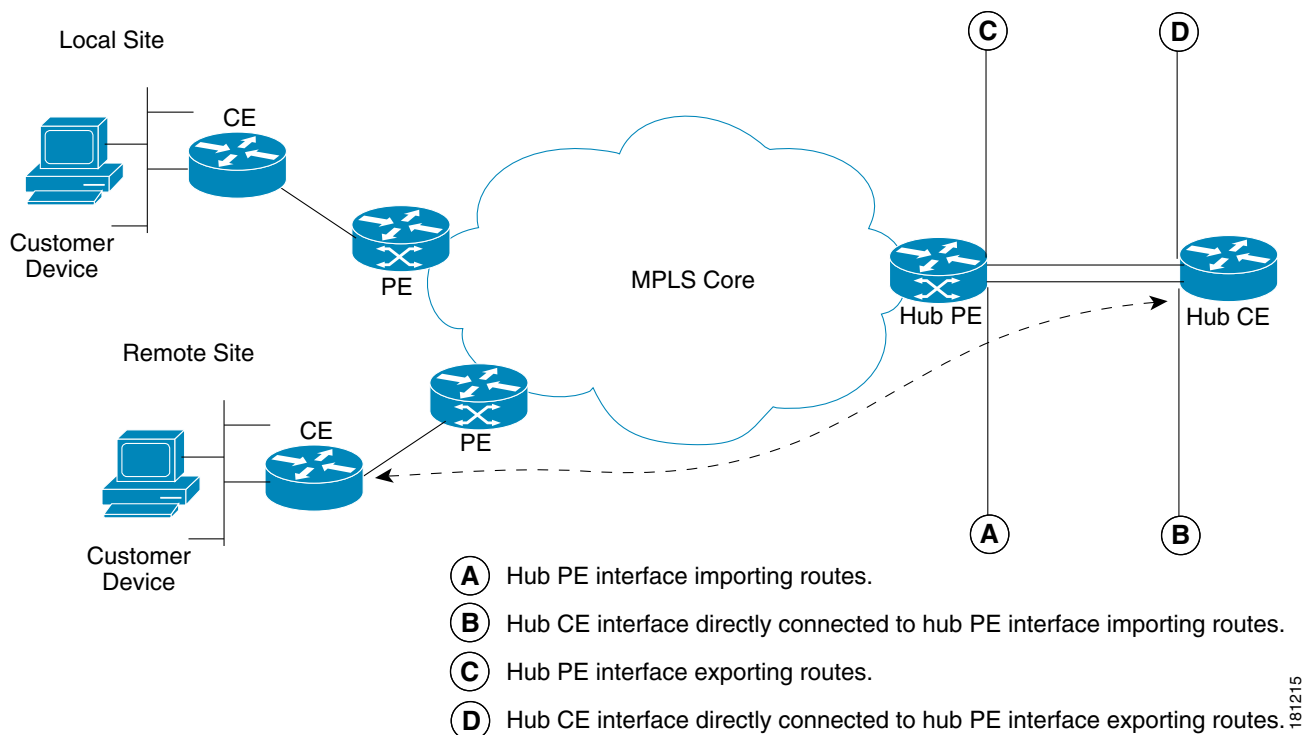
Table 11-14 **Test Configuration—Hub Route Import Interface Tests**

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.

Figure 11-29 *Testing a Hub and Spoke VPN Topology—Step 2*



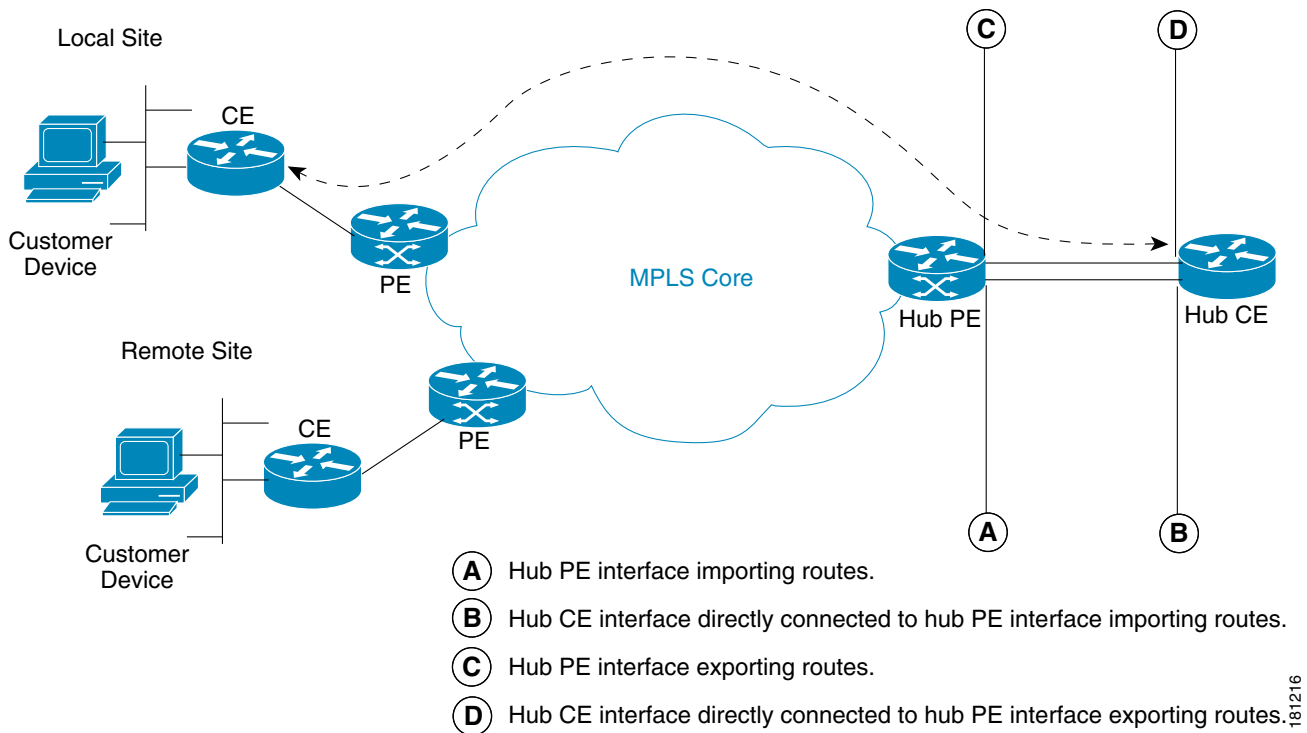
3. You should perform an MPLS VPN Connectivity Verification test between the remote site (Spoke) and the hub CE interface that is attached to the hub PE interface which imports routes (shown in [Figure 11-30](#) as *B*). When configuring the MPLS VPN Connectivity Verification test, the Local Site fields should be configured with details of the Hub PE/CE interfaces that import routes (shown in [Figure 11-30](#) as *A* and *B*), as shown in [Table 11-14](#). The Remote Site fields on the MPLS VPN Connectivity Verification Configuration window should be configured with details of the remote customer site.

Figure 11-30 Testing a Hub and Spoke VPN Topology—Step 3

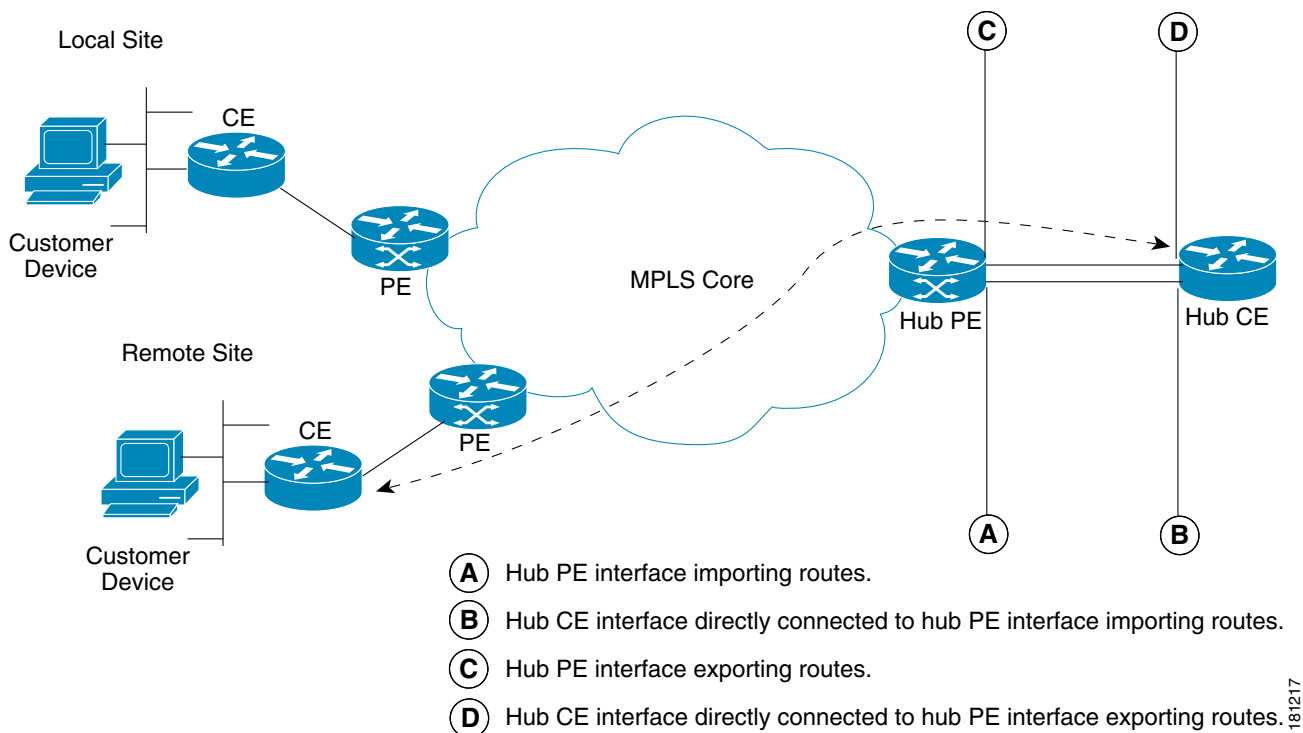
4. You should perform an MPLS VPN Connectivity Verification test between the local site (Spoke) and the hub CE interface that is attached to the hub PE interface which exports routes (shown in [Figure 11-31](#) as D). When configuring the MPLS VPN Connectivity Verification test, the Local Site fields 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 interfaces that export routes (shown in [Figure 11-31](#) as C and D), as shown in [Table 11-15](#).

Table 11-15 Test Configuration —Hub Route Export Interface Tests

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.

Figure 11-31 Testing a Hub and Spoke VPN Topology—Step 4

5. You should perform 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 in Figure 11-32 as *D*). When configuring the MPLS VPN Connectivity Verification test, the Local Site fields should be configured with details of the Hub PE/CE interfaces that export routes (shown in Figure 11-32 as *C* and *D*), as shown in Table 11-15. The Remote Site fields on the MPLS VPN Connectivity Verification Configuration window should be configured with details of the remote customer site.

Figure 11-32 Testing a Hub and Spoke VPN Topology—Step 5

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, Diagnostics will troubleshoot MPLS VPN connectivity issues including access circuit, VPN edge, and MPLS core problems. Diagnostics 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 recommends you troubleshoot the Intranet/Extranet configuration.



Note

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

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.

Failure Scenarios

This chapter provides details of all failure scenarios reported by the Diagnostics application. It also details IOS XR support caveats.

For more information, e-mail: mpls-diagnostics-expert@cisco.com



Note

Diagnostics only supports L3 services implemented on sub-interfaces/interfaces.

Failure Scenarios

This section lists the failure scenarios reported by Diagnostics, as follows:

- [Access Circuit, page 11-57](#)
- [MPLS Edge, page 11-68](#)
- [MPLS Core, page 11-74](#)
- [Customer Site, page 11-83](#)

Each failure scenario provides a table that lists whether the failure scenario is supported by each of the five Diagnostics test types. This table details whether the failure scenario is supported on IOS and IOS XR. The table also details if the failure scenario is supported for IPv4 and IPv6.



Note

In the following tables, NA stands for Not Applicable and NS stands for Not Supported.

Access Circuit

Access Circuit Blocking IP Connectivity

There is a blocking access list preventing IP connectivity from an access circuit interface on the provider (PE) router to the destination.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	Yes

An Invalid PE Interface has been Specified

Interface does not exist on the PE router.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	NA	Yes	Yes	Yes	Yes

ATM Interface Has No VPI/VCI

An asynchronous transfer mode (ATM) access circuit interface on a PE router has no virtual path identifier (VPI), or virtual channel identifier (VCI) assigned to it, or no VPI/VCI maps to the destination IP address.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

ATM Interface Is Protocol Down

An ATM access circuit interface on a PE router is protocol down. See the [“IOS XR Support” section on page 11-83](#).

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

ATM Sub-interface is Protocol Down

An ATM access circuit subinterface on a PE router is protocol down. This might be caused by incorrect subinterface parameters or by ATM Operation, Administration, and Maintenance (OAM) detecting a fault and bringing the interface down automatically. See the [“IOS XR Support” section on page 11-83](#).

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

Calculation of the CE Access Circuit Interface IP Address is only possible if the PE interface is not Unnumbered and has a /30 Subnet mask Interface on PE

Unable to calculate the customer edge (CE) access circuit interface IP address for the PE.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NA

For more details see the [“IPv6 Support” section on page 11-84](#).

eBGP Max Prefix Exceeded for Peer

Exterior border gateway protocol (eBGP) is running between the PE and CE, however the border gateway protocol (BGP) neighbor is not established. The peer has exceeded the configured maximum number of prefixes.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	Yes

eBGP Neighbor Not Established, No Route Present

eBGP is running between the PE and CE, but the BGP neighbor on the PE is not established. The BGP neighbor is on a different subnet from the PE and there is no route to the neighbor in the VPN routing/forwarding (VRF).

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	Yes

eBGP Neighbor Not Established, Possible Misconfiguration

eBGP is running between the PE and CE, but the BGP neighbor on the PE is not established. There is a route to the BGP neighbor in the VRF and it is reachable via ping. Possible CE or PE BGP configuration problem.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	Yes

eBGP Neighbor Not Established, Route Present

eBGP is running between the PE and CE, but the BGP neighbor on the PE is not established. The BGP neighbor is on a different subnet from the PE and there is a route to the neighbor in the VRF. However, the BGP neighbor is unreachable via ping.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	Yes

eBGP sites use the same AS number

The local and remote sites use eBGP and share the same AS number and neither "allowas-in" nor "as-override" is configured for the BGP neighbor within the vrf on the local PE router.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	NA	NA	NA	NA	Yes	Yes	Yes

EIGRP Not Exchanging Routes

The enhanced interior gateway routing protocol (EIGRP) is running between the PE and CE and a peer relationship has been established. However, no routes have been received from EIGRP on the CE.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

Ethernet Interface Protocol Down

An Ethernet access circuit interface on the PE router protocol is down.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	Yes

Ethernet Sub-Interface Protocol Down

An Ethernet access circuit subinterface on the PE router protocol is down.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	Yes

Frame Relay Interface Has No DLCI

A Frame Relay access circuit interface on the PE router has no data-link connection identifier (DLCI) assigned to it, or no DLCI maps to the destination IP address.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

Frame Relay Interface Protocol Down

A Frame Relay access circuit interface on the PE router protocol is down. This might be because of line parameters or cabling faults.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

Frame Relay Interface Has No DLCI

A multipoint Frame Relay permanent virtual circuit (PVC) on an access circuit interface on the PE router has no DLCI that maps to the destination IP address.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

Frame Relay Interface Has No DLCI

A point-to-point Frame Relay PVC on an access circuit interface on the PE router has no DLCI assigned to it.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

Frame Relay PVC Marked as Deleted

A Frame Relay PVC on an access circuit interface on the PE router is marked as deleted.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	NA	Yes	NS

Frame Relay PVC Marked as Down

A multipoint Frame Relay PVC on an access circuit interface on the PE router is marked as down.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	NA	Yes	NS

Frame Relay PVC Marked as Down

A point-to-point Frame Relay PVC on an access circuit interface on the PE router is marked as down.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

Incomplete Carrier on Serial Interface

A serial access circuit interface on the PE router has an incomplete carrier.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

Interface Administratively Down

An access circuit interface (or subinterface) on the PE router is administratively down.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	Yes

Interface Administratively Down

An access circuit subinterface on the PE router is administratively down.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	Yes

Interface in Protocol Down State

An access circuit interface on the PE router protocol is down.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	Yes

Interface on the PE is a Bundle Link Virtual-Access Interface

The interface on the PE is not a valid access circuit interface.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	NA	Yes	NA	Yes	NS

Interface Operationally Down

An access circuit interface on the PE router is operationally down.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	Yes

Intermittent ATM Failure (to the ATM Next Hop)

An ATM access circuit has intermittent ATM access to the ATM next hop. See the [“IOS XR Support” section on page 11-83](#).

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

Intermittent ATM Failure (to the Destination)

An ATM access circuit has intermittent ATM access to the destination. See the [“IOS XR Support” section on page 11-83](#).

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

Invalid Access Circuit IP Address Configuration

The CE router access circuit interface IP address is not in the same subnet as the attached PE access circuit interface IP address.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	Yes

Invalid Access Circuit IP Address Configuration

The CE access circuit interface IP address is a network address.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NA

For more details see the [“IPv6 Support” section on page 11-84](#).

Invalid Access Circuit IP Address Configuration

The CE access circuit interface IP address is a network broadcast address.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NA

For more details see the [“IPv6 Support” section on page 11-84](#).

Invalid Access Circuit IP Address Configuration

The CE access circuit interface IP address is the same as the attached PE access circuit interface IP address.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	Yes

IP Connectivity Problem

Unknown IP connectivity issue. An access circuit connectivity problem in the VRF instance from the PE interface to the CE.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
NA	Yes	NA	NA	NA	Yes	Yes	Yes	Yes

Missing Route

There is no route from the access circuit interface on the PE router to the destination.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	Yes

Missing Route

There is no route from the access circuit interface on the PE router to the customer destination.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	Yes

No EIGRP Peer Relationship Established

The routing protocol EIGRP is running between the PE and CE, however no peer relationship has been established.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

No EIGRP Peer Relationship Established

The routing protocol EIGRP is running between the PE and CE. The PE and CE interfaces are on different subnets and are not using IP unnumbered. No peer relationship has been established as the PE and CE are on different subnets.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

Route redistribution does not specify a route-policy

The routing protocol EIGRP is running between the PE and CE and is redistributing routes into MP-BGP. However no outbound route policy has been specified, which means all routes will be dropped rather than advertised.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	NA	Yes	Yes	NS

No OSPF Peers

Open shortest path first (OSPF) is running between the PE and CE, but no peer exists on the PE.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

OSPF not enabled on peer interface

The interface on the router does not have OPSF enabled. OSPF must be enabled on both neighboring interface.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NS	Yes	Yes	NS

OSPF in passive mode on peer interface

OSPF on interface on the router is in passive mode.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NS	Yes	Yes	NS

OSPF Area Mismatch

OSPF is enabled on the neighboring interfaces; however the interfaces are configured in different areas.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NS	Yes	Yes	NS

OSPF Area Type Mismatch

OSPF is enabled on the neighboring interfaces; however the interfaces are configured as different area types.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NS	Yes	Yes	NS

No Routing Protocol has been Determined Running between the PE and CE and no Static Route is Present

An access circuit connectivity problem in VRF.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	Yes

OSPF Not Exchanging Routes

OSPF is running between the PE and CE, but a peer relationship has been established. However, no routes have been received from OSPF on the CE.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

OSPF Peers Not Established

OSPF is running between the PE and CE, but a peer relationship has not been established.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NA

OSPF Timer Mismatch

OSPF is enabled on the neighboring interfaces; however the interfaces have different values configured for their [helloldead] timers.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NS	Yes	Yes	NS

OSPF Peers Not Established

OSPF is running between the PE and CE. However, a peer relationship has not been established as PE and CE interfaces are on different subnets and are not using IP unnumbered.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

Route redistribution does not specify a route-policy

The routing protocol OSPF is running between the PE and CE and is redistributing routes into MP-BGP. However no outbound route policy has been specified, which means all routes will be dropped rather than advertised.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	NS	Yes	Yes	NS

PE has No Route to CE

Connected PE and CE interfaces are on different subnets. No routing protocol has been determined running between the PE and CE and no static route to the CE is present.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	NA	Yes	NS

RIB Failure

A route from the PE to a destination in a VRF has not been installed in the VRF routing table. This has been identified as a Routing Information Base (RIB) failure.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	NA	Yes	NA	Yes	NS

RIP Misconfiguration

Routing information protocol (RIP) is running between the PE and CE, but no routes have been received from RIP on the CE.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

RIP Not Exchanging Routes

RIP is running between the PE and CE, but no routes have been received from RIP on the CE as the PE and CE interfaces are on different subnets and are not using IP unnumbered.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

Route redistribution does not specify a route-policy

The routing protocol RIP is running between the PE and CE and is redistributing routes into MP-BGP. However no outbound route policy has been specified, which means all routes will be dropped rather than advertised.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	NA	Yes	Yes	NS

Serial Interface in Loopback Mode

A serial access circuit interface on the PE router is configured in loopback mode.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

Serial Interface Operationally Down

A serial access circuit interface on the PE router is operationally down.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

Static IP address on ATM Point-to-Point Interface

An ATM access circuit has a static IP address mapping on an ATM point-to-point subinterface. Neither a static mapping nor an address resolution protocol (ARP) are required on a point-to-point subinterface because there is a single VC and a single path for the traffic. See the [“IOS XR Support” section on page 11-83](#).

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

Sub-interface in Protocol Down State

An access circuit subinterface on the PE router protocol is down.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	Yes

Undiagnosed ATM Failure (ATM Pings Failed but the ATM Segment Ping Succeeded)

An ATM access circuit connection is broken. The end-to-end ATM ping failed, but the ATM segment ping succeeded. This might be caused by various issues such as incorrect ATM line parameters, misconfigured ATM routing, CE or ATM cloud interfaces being down, or devices being down. See the [“IOS XR Support” section on page 11-83](#).

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

Undiagnosed ATM Failure (End to End and Segment ATM Pings Failed)

An ATM access circuit connection is broken. Both the end-to-end and segment ATM pings failed. This might be caused by various issues such as incorrect ATM line parameters, misconfigured ATM routing on the ATM next hop, next hop interfaces being down, or devices being down. See the [IOS XR Support, page 11-83](#).

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

Virtual Template Interface has been Specified for the PE Access Circuit Interface

The PE interface on the PE is not a valid access circuit interface.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	NA	Yes	NA	Yes	NS

MPLS Edge

BGP Next Hop Interface Admin Down

BGP next hop on PE is assigned to a loopback interface. However, that interface is administratively down.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes

BGP Next Hop is Not Assigned to an Interface

The BGP next hop for routes to the remote site PE is not assigned to an interface on the remote PE.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes

BGP Not Active

BGP is not active on the PE router.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	NA	Yes	Yes	Yes	Yes

BGP Peers Using Same BGP Next Hop

BGP VPNv4/VPNv6 peers use the same BGP next hop. This prevents correct route distribution of PE routes. Other routing problems might also be encountered.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	NA	Yes	Yes	Yes	Yes

BGP Peers Using Same Router Identifier (RID)

BGP VPNv4/VPNv6 peers use the same router identifier. This prevents correct route distribution of PE routes. Other routing problems might also be encountered.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Multiple Access Circuits in the same subnet

LSP Connectivity problem, control plane issue. The next-hop for the current BGP selected route(s) to the remote PE router is not assigned to an interface on the local PE router. There are multiple VPNv4/VPNv6 routes found within the vrf on the locale PE router to the remote prefix.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	NA	NA	NA	Yes	Yes	Yes	Yes

BGP to LFIB Mismatch

Untagged entry has mismatch between BGP and label forwarding information base (LFIB) tables.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	NA	Yes	Yes	Yes	Yes

BGP to FIB Mismatch

The forwarding information base (FIB) and BGP entries are inconsistent.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	NA	Yes	Yes	Yes	Yes

Duplicate BGP Next Hop

Duplicate IP address found in the network for the BGP next hop on PE.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Duplicate IP Address

There is a duplicate IP address configured on the PE router that conflicts with an access circuit interface.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	Yes

Duplicate IP Address

Duplicate IP address found in the network for the BGP router identifier on PE.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes

eBGP not Redistributing Connected Routes into MP-BGP

The routing protocol eBGP is running between the PE and CE, but eBGP on the PE is not redistributing connected routes into Multi Protocol (MP)-BGP, also there is no explicit network statement.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	Yes

FIB to LFIB Mismatch

Aggregate entry has mismatch between FIB and LFIB tables.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	Yes

Ingress FIB to Egress LFIB Mismatch

Egress LFIB and Ingress FIB inconsistency.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	NA	Yes	Yes	Yes	Yes

Inconsistent BGP Entries

BGP entries are inconsistent for the VRF.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	NA	Yes	Yes	Yes	Yes

Label mismatch or interfaces on different VPNs Down

VPN connectivity problem in VRF from PE to destination. BGP VPNv4/VPNv6 label for prefix do not match. This might indicate a label mismatch or interfaces on different VPNs. Check that the interfaces selected are on the same VRF.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
NA	NA	NA	Yes	NA	Yes	Yes	Yes	Yes

PE interface is administratively down

The access circuit interface on the PE router is administratively down.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	NS

Missing Router Identifier (RID)

Unable to determine the local router identifier on the PE.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
NA	NA	NA	NA	Yes	Yes	Yes	Yes	Yes

Missing VPNv4 Address Family Configuration

VPNv4 configuration missing; Virtual private network (VPN) label exchange problem. VPNv4 address family configuration missing from BGP router configuration on the PE router. This results in routes being dropped.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	NA	Yes	Yes	Yes	Yes

Missing VPNv6 Address Family Configuration

VPNv6 configuration missing; Virtual private network (VPN) label exchange problem. VPNv6 address family configuration missing from BGP router configuration on the PE router. This results in routes being dropped.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	NA	NA	Yes	NA	Yes

MPLS LDP Package not enabled on IOS XR Router

The MPLS LDP package is not enabled on the IOS XR router.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NA	Yes	Yes	Yes

MPLS Package installed but not active on IOS XR Router

The MPLS package is installed, but it is not active on the IOS XR router.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NA	Yes	Yes	Yes

MPLS Package not installed on IOS XR Router

The MPLS package is not installed on the IOS XR router.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NA	Yes	Yes	Yes

No MP-BGP Neighbors

There are no MP-BGP neighbors defined on the PE router.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	NA	Yes	Yes	Yes	Yes

No MP-BGP Neighbor Session Established

No MP-BGP neighbor session established on the PE router.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	NA	Yes	Yes	Yes	Yes

No VPN Label For Prefix

No VPN label has been allocated for the prefix.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	NA	Yes	Yes	Yes	Yes

No VRF Associated with PE Interface

An interface on the PE router has no VRF associated.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	NA	Yes	Yes	Yes	Yes

OSPF Loopback Interface Uses A Non /32 Netmask

VPNv4 routes are being advertised to IBGP neighbors by the PE. The address of the next hop is a loopback interface that does not have a /32 mask defined. OSPF is being used on this loopback interface, and the OSPF network type of this interface is loopback. OSPF advertises this IP address as a host route (with mask /32), regardless of what mask is configured. This advertising conflicts with TDP/LDP, that uses configured masks, so the TDP/LDP neighbors might not receive a label for the routes advertised by this router. This condition could break connectivity between sites that belong to the same VPN.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	NA	Yes	NA

PE Interface Has No IP Address

An interface on the PE router has no IP address.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	NA	Yes	Yes	Yes	Yes

Router ID Loopback Interface Down

The loopback interface used to assign the local router ID on the PE is administratively down.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	Yes

Routes not Redistributed to or from MP-BGP

Routes are not being redistributed to or from MP-BGP on the PE.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	NA	Yes	NA

Static Route to Remote Prefix

A static route to a remote prefix has been configured within a VRF on the PE.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	NA	Yes	Yes	Yes	Yes

Traffic Administratively Blocked

VPN connectivity problem from the PE to the destination due to traffic being administratively blocked.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	NA	NA	Yes	Yes	Yes	Yes

Troubleshooting of the Layer 3 VPN has been Unable to Find the Cause of the Failure

LSP connectivity problem.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Troubleshooting of the Layer 3 VPN has been Unable to Find the Cause of the Failure

VPN connectivity problem in VRF from PE to destination.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	NA	Yes	Yes	Yes	Yes

VRF Route Target Import/Export Mismatch

VRF route target import/export mismatch between the PE devices.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	NA	Yes	Yes	Yes	Yes

MPLS Core

An Invalid PE Interface has been Specified

Interface supplied as the LSP Endpoint does not exist on the PE router.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
NA	NA	NA	NA	Yes	Yes	Yes	Yes	NA

Broken LDP Neighbor Session

LDP session with downstream neighbor broken. Route processor/line card forwarding discrepancy on the router. See the [“IOS XR Support” section on page 11-83](#).

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	NA	Yes	Yes

CEF Not Enabled On Router

CEF has not been enabled on a router. See the [“IOS XR Support” section on page 11-83](#).

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	NA	Yes	Yes

Distributed LFIB Table Discrepancy

There is a discrepancy in the LFIB table between the route processor and line cards.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	NA	Yes	Yes	Yes	Yes

Distributed FIB Table Discrepancy

There is a discrepancy in the FIB table between the route processor and line cards.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	NA	Yes	Yes	Yes	Yes

Label Inconsistency

LFIB local tag, received packet, and LDP local binding label inconsistent on the router. See the [“IOS XR Support” section on page 11-83](#).

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	NA	Yes	Yes

LDP Host Not Reachable

The host is not reachable from the label switch router (LSR). This could be caused by no LDP session on router for the downstream router, LDP ID not reachable because of IGP problem, ACL configured that is blocking LDP packets, or an authentication problem.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes

LDP Label Mismatch

Label received for a prefix did not match the label sent. See the [“IOS XR Support” section on page 11-83](#).

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	NA	Yes	Yes

LDP Neighbors Not Discovered

LDP neighbors have not been discovered. Generic LDP discovery problem found on an interface of the device with its downstream neighbor. See the [“IOS XR Support” section on page 11-83](#).

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	NA	Yes	Yes

LDP Neighbors Not Discovered

LDP neighbors have not been discovered. An interface on a router has an ACL configured that could be preventing LDP neighbor discovery.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes

LDP Neighbors Not Established

LSP connectivity problem, control plane issue. The LDP session is not established. The interface has an ACL configured that could be blocking LDP session establishment on port 646.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes

LDP/TDP Mismatch

LDP and TDP have been enabled on opposite ends of a link. See the [“IOS XR Support” section on page 11-83](#).

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes

LSP Reply Path Problem

LSP connectivity problem with the reply path. See the [“IOS XR Support” section on page 11-83](#).

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	NA	Yes	Yes

Missing LFIB Entry

LFIB entry missing. Could be because of misrouting in an earlier router, or due to duplicate loopbacks. See the [“IOS XR Support” section on page 11-83](#).

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	NA	Yes	Yes

Missing or Untagged Return Path

Return path from the core router absent or untagged for the prefix. See the [“IOS XR Support” section on page 11-83](#).

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	NA	Yes	Yes

MPLS Label Space Exhausted

MPLS label space exhausted on a router.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes

MPLS Not Enabled Globally

MPLS has not been enabled globally on router.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	NA	Yes	Yes

MPLS Not Enabled On Interface

MPLS has not been enabled on an interface. See the [“IOS XR Support” section on page 11-83](#).

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes

No Entry for Label

No entry in LFIB for incoming label going to the destination prefix. See the [“IOS XR Support” section on page 11-83](#).

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	NA	Yes	Yes

No LDP Session with Neighbor

No LDP session on router exists with neighbor.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes

No Valid Next-Hop Entry

No valid entry can be found for the next-hop from the current device. See the [“IOS XR Support” section on page 11-83](#).

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	NA	Yes	Yes

Routing Loop In Forwarding Path

A routing loop is present in the forwarding path.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes

All MPLS enabled core facing interfaces are down

LSP connectivity problem, control plane issue. No MPLS enabled interface is operationally up.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Label Advertising Not Enabled

Label advertisement is disabled on router.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Label Advertising Possibly Denied by ACL

Label advertisement has been globally disabled, but selectively enabled for one or more access lists. The ACL(s) might be denying the advertising of labels to the destination prefix.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes

TTL Propagation Disabled

Could not troubleshoot or detect failure point because the device is not propagating the Time To Live (TTL).

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Check tunnel traffic admission policy

No traffic admission policy (such as via autoroute announce, or Policy Based Tunnel Selection (PBTS) or a static route) configured on the TE Tunnel.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NA	Yes	Yes	Yes

Check if MPLS is enabled on the tunnel interface

Incomplete configuration detected for the MPLS TE Tunnel interface.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	NA	Yes	NS	Yes	Yes	Yes

Check that the primary and backup tunnel's interfaces are up

The tunnel interface on the router is administratively down.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NS	Yes	Yes	Yes

Tunnel config not present at headend

The TE Tunnel configuration is not present at the headend router.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NS	Yes	Yes	Yes

Check that the tunnels outgoing interface is operational

The outgoing interface of FRR primary tunnel configured on the router is operationally down.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NS	Yes	Yes	Yes

TE not enabled globally on router

MPLS Traffic Engineering is not enabled globally on the router.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NS	Yes	Yes	Yes

TE not enabled globally on the interface

MPLS Traffic Engineering is not enabled on the interface of the router.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NS	Yes	Yes	Yes

No IP Address assigned for tunnel

MPLS Traffic Engineering Tunnel has no IP address assigned.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NS	Yes	Yes	Yes

Tunnel destination invalid

The destination address configured for the tunnel is unreachable.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NS	Yes	Yes	Yes

Tunnel is administratively shut down

Tunnel has been admin shut down on the router.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NS	Yes	Yes	Yes

Missing OSPF configuration for TE

Router has not configured OSPF for MPLS TE.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NS	Yes	Yes	Yes

Node is not advertising MPLS TE links

Router is not advertising itself through OSPF as an MPLS TE link.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NS	Yes	Yes	Yes

No targeted LDP session exists between peer PE's

Remote Site PE router is not accepting targeted LDP session requests.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	NA	Yes	NS	Yes	Yes	Yes

Blocking ACL causing targeted LDP session setup problem

Router has an access control list which is blocking LDP messages (on TCP port 646).

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NS	Yes	Yes	Yes

Targeted LDP not established/operational between PE's

LDP has been unable to establish a targeted session between the devices due to peer PE router being unreachable.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NS	Yes	Yes	Yes

Tunnel Connectivity Failure No Targeted LDP Configuration

LDP discovery failure for the neighbor devices. The tunnel tail end device is not accepting LDP targeted hellos.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes

For link protection, check that the backup tunnel does not pass through the protected interface

There is a FRR backup tunnel configured on the router. It is configured to protect a link on router (as NHOP), which is on the path the primary tunnel takes. However the configured backup tunnel is configured to traverse this link.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NS	Yes	Yes	Yes

Check the primary tunnel has FRR enabled with 'fast-reroute'

A tunnel has been detected on router. It appears that this tunnel is intended to be a primary tunnel, but it does not have the fast-reroute configuration as required.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	NA	Yes	NS	Yes	Yes	Yes

Node protection - Check if backup tunnel path is explicit and does not contain the protected node interface in path

There is a FRR backup tunnel configured on router. It is configured to protect a router (as NNHOP), which is on the path the primary tunnel takes. However the configured backup tunnel is configured to traverse a link on this router.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NS	Yes	Yes	Yes

Check if the primary & backup tunnel merge point is reachable

The merge point router for FRR primary tunnel and FRR backup tunnel is unreachable.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NS	Yes	Yes	Yes

TE ping failure

The *ping mpls traffic-eng tunnel* command returned failure.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	NA	Yes	NS	Yes	Yes	Yes

Tunnel operationally down

The *show mpls traffic-eng tunnels* command has indicated that the TE Tunnel is down.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	NA	Yes	NS	Yes	Yes	Yes

Tunnel Connectivity Failure

Unknown MPLS TE connectivity problem.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	NA	Yes	Yes	Yes

Unable to Troubleshoot MPLS TE Connectivity Problem

Router is running a non-OAM Cisco IOS version. The connectivity of the tunnel cannot be tested.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Unknown LSP Connectivity Problem

LSP connectivity problem, data plane issue, or unknown cause.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Unsupported IOS Version

Core router running an unsupported IOS version. This version of IOS does not support the required OAM functionality.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	NA	Yes	Yes	Yes	Yes	NA	Yes	NS

VPN Connectivity Tests have been Exercised and No Failures Found (However as Pings are Blocked to the CE, it is Not Possible to Verify VPN Connectivity)

Unable to verify VPN connectivity in VRF from PE to destination.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Customer Site**Possible Customer Routing Issue**

The PE has some routes from the CE, but the CE is unable to respond to pings.

CE to CE	PE to Attached CE	CE to PE Across Core	PE to PE (in VRF)	PE to PE Core	IOS	IOS XR	IPv4	IPv6
Yes	Yes	Yes	NA	NA	Yes	Yes	Yes	Yes

IOS XR Support

This section details the IOS XR support caveats:

1. [MPLS Not Enabled On Interface, page 11-77](#)

IOS XR has the concept of packages. One of the packages relevant to Diagnostics is the MPLS package. When Diagnostics troubleshooting focuses on an IOS XR router in the core, various preparation checks are carried out to ensure that the router is configured sufficiently; that is, that the MPLS package is installed and active, and then to check for the required features being enabled (MPLS OAM and MPLS LDP). If any of these checks fail, a failure scenario is reported. [MPLS Not Enabled On Interface, page 11-77](#) remains valid for IOS devices, or when MPLS is disabled on an interface on an IOS XR device.

2. [CEF Not Enabled On Router, page 11-75](#)

It is still possible for Diagnostics to determine cases where CEF is disabled on IOS routers in the core, for example, CEF could be disabled via CLI configuration, or when the router is overloaded and shuts itself down. In such cases, the IOS CLI command **show cef state** reports that CEF is either *enabled/running* or *disabled/not running*, and Diagnostics can determine that CEF is disabled.

CEF cannot be disabled on an IOS XR router. When the CEF switching feature on an IOS XR router becomes overloaded, it does not shut down. Instead, it applies back pressure to the queue of outstanding requests in an effort to reduce the load on the CEF switching process. Therefore, in an IOS XR router, the relevant CLI **show** command does not report that CEF is non-operational, and thus this failure scenario is not valid on an IOS XR router.

3. [LDP/TDP Mismatch, page 11-76](#)

This is not a valid scenario where directly connected IOS XR routers are present, because IOS XR only supports a single label distribution protocol – that is LDP. It is possible for the application to find LDP-TDP mismatch if it is configured in IOS-IOS XR, IOS XR-IOS, or IOS-IOS configurations.

4. [Broken LDP Neighbor Session, page 11-74](#)

[Label Inconsistency, page 11-75](#)

[LDP Label Mismatch, page 11-75](#)

[LDP Neighbors Not Discovered, page 11-76](#)

[LSP Reply Path Problem, page 11-76](#)

[Missing LFIB Entry, page 11-76](#)

[Missing or Untagged Return Path, page 11-77](#)

[No Entry for Label, page 11-77](#)

[No Valid Next-Hop Entry, page 11-78](#)

These failure scenarios are due to specific bugs in IOS versions, and are not applicable to IOS XR.

5. [ATM Interface Is Protocol Down, page 11-58](#)

[ATM Sub-interface is Protocol Down, page 11-58](#)

[Intermittent ATM Failure \(to the ATM Next Hop\), page 11-62](#)

[Intermittent ATM Failure \(to the Destination\), page 11-62](#)

[Static IP address on ATM Point-to-Point Interface, page 11-67](#)

[Undiagnosed ATM Failure \(ATM Pings Failed but the ATM Segment Ping Succeeded\), page 11-68](#)

[Undiagnosed ATM Failure \(End to End and Segment ATM Pings Failed\), page 11-68](#)

These failures are not supported in case of ATM interfaces on the CRS-1 platform. However, they continue to be applicable on IOS devices and for IOS XR on the Cisco 12000 XR Series.

IPv6 Support

This section details the IPv6 support caveats:

- In addition to IPv4 troubleshooting for both IOS and IOS XR devices, troubleshooting is extended for the IOS XR devices where IPv6 addressing is used on the PE-CE link. IPv6 is not supported on IOS devices.
- Ethernet is the only Access Circuit interface technology on which Diagnostics can troubleshoot, when IPv6 addressing is used on IOS XR devices.

- IPv6 support is extended only to support eBGP as the PE-CE routing protocol.
- Since the scope of the IPv6 address is only between the attachment circuit links, it is assumed that both ends of the LSP to have either IPv6 or IPv4 and not IPv6 at one end and IPv4 at the other and vice-versa.
- IPv6 support can troubleshoot PE-CE links configuration with Global Unicast IPv6 address alone.
- For IPv6 support, IPv4 router-id will be used for identification of Peer Routers, for protocols including BGP and LDP.
- Unlike in case of IPv4, the CE Access Circuit Interface IP address (for applicable test types) will not be auto populated as IPv6 unnumbered is not supported on IOS XR devices and there is no concept of /30 and /31 address in IPv6.
- The below failure scenarios although applicable on IOS XR, not applicable in IPv6 context as these validations are performed during initial data validations. The failure scenario to report that the CE access circuit interface IP address is a network address is performed during initial data validations. There is no concept of Broadcast address in IPv6.
 - Broadcast Address
 - Network Address

Observations

Observations are conditions that could lead to connectivity problems. Because Diagnostics cannot categorically conclude the cause of the connectivity problem, these conditions are reported as observations.

For more information, e-mail: mpls-diagnostics-expert@cisco.com

ACL Configured on PE

There is an access control list (ACL) configured on the provider edge (PE) router. It might be causing failure of the VPN routing/forwarding instance (VRF) ping from this PE to the remote PE, however we have not analyzed the ACL to confirm its usage. This is not causing the connectivity failure from the PE to the local customer edge (CE) router, or customer device.

BGP Neighbor Session Problem

Possible border gateway protocol (BGP) neighbor session problem detected. Displays table with columns BGP Neighbor (Neighbor IP Address) and BGP State (BGP Neighbor State).

BGP Router ID is Not a Loopback Interface

The local BGP router ID on the PE is not assigned to a loopback interface. It is recommended that the router ID is taken from a loopback interface to both reduce the chance of duplication and enhance stability.

Connected Routes Not Redistributed into MP-BGP

Directly connected routes might not be redistributed into MP-BGP.

Core Troubleshooting Could Not be Performed. The VPN Route is External.

Core troubleshooting could not be performed. Diagnostics is unable to determine the label-switched path (LSP) to test, because the PE *<PE Name>* has no valid VPN route to the remote prefix *<IP address>* within the VRF *<VRF name>*. The route is not learned through an internal Border Gateway Protocol (BGP) VPNv4 neighbor. It is known through the *<Routing Protocol Name>*. The next-hop for this external route is *<IP address>*. Traffic does not flow through the MPLS core, as expected. This might be an intentional back door link, however, it is often a symptom of PE - CE misrouting. To test LSP connectivity, you might want to run a PE to PE Core test that allows you to specify the LSP endpoints manually.

Core Troubleshooting Could Not be Performed. The VPN Route is External and the Next-Hop Is Inaccessible.

Core troubleshooting could not be performed. Diagnostics is unable to determine the LSP to test, because the PE *<PE Name>* has no valid virtual private network (VPN) route to the remote prefix *<IP address>* within the VRF *<IP address>*. The route is not learned through an internal BGP VPNv4 neighbor. It is known through the *<Routing Protocol Name>*. The next-hop for this external route is inaccessible. This might be an intentional back door link, however, it is often a symptom of PE - CE misrouting. To test LSP connectivity, you might want to run a PE to PE Core test that allows you to specify the LSP endpoints manually.

Core Troubleshooting Could Not be Performed. The VPN Route Next-Hop is Inaccessible.

Core troubleshooting could not be performed. Diagnostics is unable to determine the LSP to test, because the PE *<PE Name>* has no valid VPN route to the remote prefix *<IP address>* within the VRF *<VRF name>*. The next-hop is inaccessible. This might be due to a problem within the Core Interior Gateway Protocol (IGP) or IP connectivity failure. To test LSP connectivity, you might want to run a PE to PE Core test that allows you to specify the LSP endpoints manually.

Duplicate BGP Router ID

BGP Router Identifier on the PE is found to be duplicated on one or more interfaces of the listed devices.

eBGP Maximum Prefixes

The exterior border gateway protocol (eBGP) session between the PE and an eBGP neighbor has a maximum prefix count configured on the PE. There are currently *X* prefixes in the VRF from this neighbor.

eBGP Neighbor Not Established

It appears that you are running eBGP as your PE-CE routing protocol. The PE and CE interfaces are on different subnets and there is no route to the CE on the PE. Until there is a route to the CE, this eBGP session is not established.

eBGP Neighbors Not Established

eBGP neighbors have been specified in a VRF but are not established and are unreachable.

EIGRP Peer Relationship Not Established

The PE interface is configured with IP unnumbered. The CE interface must either also be using IP unnumbered or be on the same subnet in order for the enhanced interior gateway routing protocol (EIGRP) to establish a peer relationship.

Full-Mesh VPN Topology

These routers appear to be connected via a fully meshed VPN configuration. If this is not correct, there is an issue with the route target configuration.

Hub and Spoke VPN Topology

These routers appear to be connected via a hub and spoke VPN configuration. If this is not correct, there is an issue with the route target configuration.

Hub To Hub, Hub and Spoke VPN Topology

These routers appear to be connected via a hub to hub, hub and spoke VPN configuration. If this is not correct, there is an issue with the route target configuration.

Incomplete CEF Adjacencies

Incomplete Cisco express forwarding (CEF) adjacencies on the access circuit interface.

Incorrect Multilink Virtual-Access Interface Specified

If you are specifying a multilink access circuit interface for the PE ensure that the virtual access interface specified is an active multilink bundle interface and that it has active bundle links.

Interface Not In VLAN

Warning: Ethernet access circuit interface is not associated with a virtual LAN (VLAN).

Intermittent Ping Success

The ping showed only intermittent connectivity.

Inverse ARP Disabled on FR Interface

The Frame Relay interface is dynamically configured but has inverse address resolution protocol (ARP) explicitly disabled.

Inverse ARP Implicitly Disabled on FR Interface

There is a Frame Relay static map on the interface. This interface is configured dynamically but the presence of the static map will, as a side effect, disable inverse ARP.

LMI Disabled on Frame Relay Interface

Warning: Frame Relay permanent virtual circuit (PVC) status cannot be checked on interface because the local management interface (LMI) is disabled.

LSP Endpoint is Not a Loopback Interface

The VPNv4 route is being sent to IBGP neighbor(s). However, the next hop address is one of the directly connected physical interfaces. It is recommended to use loopback interfaces as the next hops for VPNv4 IBGP neighbors. If the address is not available at the correct hop via the IGP, it could break connectivity between VPN sites because no forwarding label information is available.

MPLS OAM Package is not enabled on IOS XR Router

MPLS OAM package is not enabled on the IOS XR router.

MPLS TE Package is not Enabled on IOS XR Router

MPLS TE package is not enabled on the IOS XR router.

Multiple Equal Cost Paths

Equal cost multiple paths (ECMP) were found.

Non-compliant IOS Version on PE Router

Core troubleshooting could not be performed because the provider edge (PE) router is running a non MPLS OAM compliant Cisco IOS version.

No Routes Received from eBGP

It appears that you are running eBGP as your PE-CE routing protocol. However, no routes have been received from the neighbor.

No Route to Remote Prefix Received from eBGP

It appears that you are running eBGP as your PE-CE routing protocol. However, the route to a remote prefix has not been received from the neighbor. Check PE and customer edge (CE) BGP configuration.

No VPN Label in VRF for Prefix

No virtual private network (VPN) label was found for the address in the VPN routing/forwarding (VRF) on the device.

OSPF Peer Relationship Not Established

The PE interface is configured with IP unnumbered. The CE interface must either also be using IP unnumbered or be on the same subnet in order for open shortest path first (OSPF) to establish a peer relationship.

PE-PE Core Only Test Performed and the Optional Loopback IP Address Parameters Have Not Been Supplied

The LSP under test was selected based on the BGP router-id of the remote site PE. If the network has multiple LSPs between the two PEs, the reported result might not accurately reflect the state of the LSP used for customer traffic. To ensure the correct LSP is tested, you can supply the LSP endpoints on the test input window.

Possible Backup Link

The ping from the PE to the destination prefix succeeded, however the route from the PE to the destination prefix has not been learned via the expected PE interface. There might be a backup link in operation, or you might have input the incorrect parameters.

Possible Blocking Route Map

A route map is configured on the PE which might be causing route traffic to be lost. If this is an intranet/extranet VPN configuration, then there might be a route map configuration error.

Possible Core IP Failure

The internet control message protocol (ICMP) ping issued from the local PE to the remote PE failed. There is no route to the remote PE in the Interior Gateway Protocol (IGP) route table of the local PE. Try troubleshooting IP connectivity between these devices.

Possible Ethernet Duplex Mismatch

Warning: Access circuit interface has late collisions. This might be caused by an Ethernet duplex mismatch.

Route Limit Reached

The route count on the device has reached the route limit.

Traceroute Not Transmitted

The MPLS traceroute was not transmitted.

This chapter provides details of all IOS and IOS XR commands executed by the troubleshooting workflow in the Diagnostics application for the Cisco Prime Provisioning 6.3 release.

IOS Commands

This section lists the IOS commands used by Diagnostics. If TACACS+ (or another authentication/authorization system) is used, ensure that these are all allowed for Diagnostics.



Note

This list might be updated when Diagnostics releases or patches are made available, e-mail: mpls-diagnostics-expert@cisco.com for the latest list.

1. attach *<slot>* show version
2. execute-on slot *<slot>* 'show mpls forwarding-table *<destinationPrefix>* *<subnetMask>*'
3. execute-on slot *<slot>* 'show mpls forwarding-table *<destinationPrefix>*'
4. execute-on slot *<slot>* 'show mpls forwarding-table vrf *<vrfName>* *<destinationPrefix>* *<subnetMask>*'
5. execute-on slot *<slot>* 'show mpls forwarding-table vrf *<vrfName>* *<destinationPrefix>*'
6. execute-on slot *<slot>* 'show mpls forwarding-table vrf *<vrfName>*'
7. execute-on slot *<slot>* 'show mpls forwarding-table'
8. execute-on slot *<slot>* show ip cef vrf *<vrfName>* *<networkPrefix>*
9. execute-on slot *<slot>* show ip cef vrf *<vrfName>* *<networkPrefix>* *<subnetMask>*
10. execute-on slot *<slot>* show version
11. ping (interactive)
12. ping *<targetIp>*
13. ping mpls ipv4 *<targetIp>*/*<targetIpSubnetMask>* source *<source>* sweep *<minSweepSize>* *<maxSweepSize>* *<sweepInterval>* *<repeatCount>* timeout *<timeout>* replyMode *<replyMode>*
14. ping mpls traffic-eng Tunnel *<tunnelNumber>*
15. ping vrf *<vrfName>* (interactive)
16. show access-lists *<listName>*
17. show atm map
18. show atm pvc *<interface>*
19. show cef drop
20. show cef drop | include ^*<slot>*
21. show frame-relay lmi
22. show frame-relay lmi interface *<interface>*
23. show frame-relay map
24. show frame-relay pvc *<interface>* dlci *<dlci>*
25. show interfaces *<interface>*
26. show ip bgp summary
27. show ip bgp vpnv4 *<vrfName>* rib-failure

28. show ip bgp vpnv4 all neighbors
29. show ip bgp vpnv4 all neighbors <destIp>
30. show ip bgp vpnv4 all | include local router
31. show ip bgp vpnv4 vrf <vrfName> <networkPrefix>
32. show ip bgp vpnv4 vrf <vrfName> neighbors <destIp>
33. show ip bgp vpnv4 vrf <vrfName> <prefix> <subnetMask>
34. show ip bgp vpnv4 vrf <vrfName> labels | include <networkPrefix>/<subnetMask> |
[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+
35. show ip bgp vpnv4 vrf <vrfName> labels | include <classfulPrefix>
36. show ip bgp vpnv4 vrf <vrfName> labels | include <networkPrefix>/<subnetMask>
37. show ip cef <destinationPrefix>
38. show ip cef summary
39. show ip cef vrf <vrfName> <networkPrefix> <subnetMask> detail
40. show ip cef vrf <vrfName> <networkPrefix> detail
41. show ip cef vrf <vrfName> adjacency <interface> <destip> detail
42. show ip eigrp <vrfName> interfaces <vrfInterface>
43. show ip interface <interface>
44. show ip interface <interface> | include access list is
45. show ip interface brief <interface>
46. show ip interface brief | include <ip-address>
47. show ip ospf <processId> <area> interface <intName>
48. show ip ospf mpls traffic-eng link
49. show ip protocols <vrfName>
50. show ip route <targetIp>
51. show ip route vrf <vrfName> <targetIp>
52. show ip traffic
53. show ip vrf detail <vrfName>
54. show ip vrf interfaces <vrfName>
55. show mpls forwarding-table <destinationPrefix>
56. show mpls forwarding-table <destinationPrefix> <subnetMask>
57. show mpls forwarding-table <destinationPrefix> detail
58. show mpls forwarding-table labels <label>
59. show mpls forwarding-table labels <label> detail
60. show mpls forwarding-table vrf <vrfName>
61. show mpls forwarding-table vrf <vrfName> <destinationPrefix>
62. show mpls forwarding-table
63. show mpls interfaces <interface>
64. show mpls interfaces all

65. show mpls ip binding <destinationPrefix> <destinationMask>
66. show mpls ip binding local
67. show mpls ip binding summary
68. show mpls label range
69. show mpls ldp bindings <ip> <subnetMask>
70. show mpls ldp bindings neighbor <neighbor ip> <subnetMask>
71. show mpls ldp discovery
72. show mpls ldp neighbor
73. show mpls ldp neighbor <interface>
74. show mpls traffic-eng tunnels
75. show mpls traffic-eng tunnels <status>
76. show mpls traffic-eng tunnels <tunnelId>
77. show mpls traffic-eng tunnels destination <destination> <status>
78. show mpls traffic-eng tunnels destination <destination>
79. show mpls traffic-eng tunnels role <role>
80. show mpls traffic-eng tunnels role <role> <status>
81. show mpls traffic-eng tunnels role <role> destination <destination> <status>
82. show mpls traffic-eng tunnels role <role> destination <destination> up
83. show mpls traffic-eng tunnels role head brief
84. show ppp multilink interface <interface>
85. show route-map <mapName>
86. show running-config
87. show running-config interface <interface>
88. show running-config interface <interface> | include frame-relay interface-dlci
89. show running-config interface <interface> | include map-group
90. show running-config interface <interface> | include no frame-relay inverse-arp
91. show running-config | begin router bgp
92. show running-config | include advertise-
93. show running-config | include ldp password
94. show running-config | include mpls label protocol
95. show running-config | include no
96. show version
97. show vlans
98. traceroute mpls ipv4 <ipAddress>/<subnetMask> source <source> destination <destination> ttl 15
99. traceroute mpls traffic-eng Tunnel <tunnelNumber>
100. traceroute vrf <vrfName> (interactive)

IOS XR Commands

This section lists the IOS XR commands used by Diagnostics. If TACACS+ (or another authentication/authorization system) is used, ensure that these are all allowed for Diagnostics.



Note

This list might be updated when Diagnostics releases or patches are made available, e-mail: mpls-diagnostics-expert@cisco.com for the latest list.

1. ping <targetIp>
2. ping atm interface <interface> <vpi>/<vci>
3. ping atm interface <interface> <vpi>/<vci> end-loopback
4. ping atm interface <interface> <vpi>/<vci> seg-loopback
5. ping mpls ipv4 <destination>/<subnetMask>
6. ping mpls ipv4 <destination>/<subnetMask> reply mode router-alert
7. ping mpls ipv4 <destination>/<subnetMask> source <source>
8. ping mpls traffic-eng Tunnel <tunnelId>
9. ping vrf <vrfName>
10. ping vrf <vrfName> <targetIp> <sourceInterface> <minSweepSize> <maxSweepSize> <sweepInterval>
11. show access-lists ipv4 <listName>
12. show bgp ipv4 all summary
13. show bgp vpnv4 unicast neighbors
14. show bgp vpnv4 unicast summary
15. 14.show bgp vpnv4 unicast vrf <vrfName> <networkPrefix>
16. show bgp vpnv4 unicast vrf <vrfName> <prefix> <mask>
17. show bgp vpnv4 unicast vrf <vrfName> labels
18. show bgp vrf <vrfName> advertised neighbor <neighboreId> summary | include <ceDeviceIpAddr>
19. show bgp vrf <vrfName> ipv4 unicast
20. show bgp vrf <vrfName> neighbors
21. show bgp vrf <vrfName> vpnv4 unicast neighbors
22. show cef ipv4 <destinationPrefix>
23. show cef ipv4 drops
24. show cef ipv4 drops location <slot>
25. show cef ipv4 summary
26. show cef vrf <vrfName> ipv4 <networkPrefix> detail
27. show cef vrf <vrfName> ipv4 <networkPrefix> <subnetMask> detail
28. show cef vrf <vrfName> <networkPrefix> <subnetMask> location <location>
29. show eigrp <vrfName> interfaces <vrfInterface>

30. show frame-relay lmi
31. show frame-relay lmi interface <interface>
32. show install active summary
33. show install inactive summary
34. show install location <slot>
35. show interfaces <interface>
36. show ip cef vrf <vrfName> adjacency <interface> <destip> detail
37. show ip ospf <processId> <area> interface <intName>
38. show ipv4 interface <interface>
39. show ipv4 interface brief <interface>
40. show ipv4 interface brief | include <ip-address>
41. show ipv4 traffic
42. show ipv4 vrf <vrfName> interface brief
43. show ipv4 vrf <vrfName> interface <interface>
44. show ipv4 vrf all interface brief
45. show mpls forwarding
46. show mpls forwarding labels <label>
47. show mpls forwarding prefix <destinationPrefix>/<subnetMask>
48. show mpls forwarding prefix <destinationPrefix>/<subnetMask> detail
49. show mpls forwarding vrf <vrf>
50. show mpls forwarding vrf <vrf> prefix <destinationPrefix>/<subnetMask>
51. show mpls forwarding vrf <vrfName> prefix <destinationPrefix>/<subnetMask> labels <label> location <location>
52. show mpls forwarding vrf <vrfName> prefix <destinationPrefix>/<subnetMask> location <location>
53. show mpls interfaces
54. show mpls interfaces <interface>
55. show mpls label range
56. show mpls label table summary
57. show mpls ldp bindings <ip> <mask>
58. show mpls ldp bindings neighbor <neighbor> <ip> <mask>
59. show mpls ldp discovery
60. show mpls ldp neighbor
61. show mpls ldp neighbor <interface>
62. show mpls traffic-eng tunnels
63. show mpls traffic-eng tunnels backup <tunnelId>
64. show mpls traffic-eng tunnels brief role head
65. show mpls traffic-eng tunnels <status> detail

66. show mpls traffic-eng tunnels < tunnel-id >
67. show mpls traffic-eng tunnels < tunnelNumber > detail
68. show mpls traffic-eng tunnels destination < destination >
69. show mpls traffic-eng tunnels name < name >
70. show mpls traffic-eng tunnels destination < destination > < status > detail
71. show mpls traffic-eng tunnels destination < destination > detail
72. show mpls traffic-eng tunnels detail
73. show mpls traffic-eng tunnels role < role > < status > detail
74. show mpls traffic-eng tunnels role < role > destination < destination > < status > detail
75. show mpls traffic-eng tunnels role < role > destination < destination > up detail
76. show mpls traffic-eng tunnels role < role > detail
77. show ospf
78. show ospf vrf < vrf >
79. show ospf border-routers | include ABR
80. show ospf | include ID
81. show ospf mpls traffic-eng link
82. show ospf vrf < vrfName > interface brief
83. show ospf vrf < vrfName > interface < interfaceName >
84. show protocols | include OSPF
85. show rib ipv4 tables
86. show rib vrf < vrf > ipv4 unicast statistics < protocolName >
87. show rib vrf < vrf > protocols
88. show rip vrf < vrf >
89. show route ipv4 < targetIp >
90. show route vrf < vrfName > ipv4 < targetIp >
91. show rpl route-policy < mapName >
92. show rsvp neighbors
93. show running-config
94. show running-config explicit-path name < explicitPathName >
95. show running-config interface < interface >
96. show running-config mpls ldp
97. show running-config mpls ldp label advertise
98. show running-config mpls traffic-eng
99. show running-config router bgp
100. show running-config router bgp < asNumber > vrf < vrfName > neighbor < neighborIpAddr >
101. show running-config router bgp < asNumber > neighbor-group < neighborGroupName >
102. show running-config router bgp | include redistribute < protocol >
103. show running-config router ospf

104. show running-config router <protocol ID> vrf <vrf>
105. show running-config rsvp interface <interface-name>
106. show vlan interface
107. show version
108. show vrf <vrfName> ipv4 detail
109. traceroute mpls ipv4 <destination>/<subnetMask>
110. traceroute mpls traffic-eng Tunnel <tunnelId>
111. traceroute vrf <vrf>
112. ping vrf <vrfName> <targetIpv6Address> <sourceInterface> <minSweepSize> <maxSweepSize> <sweepInterval>
113. show bgp vpnv6 unicast neighbors
114. show bgp vpnv6 unicast neighbors <destIp>
115. show bgp vpnv6 unicast vrf <vrfName> <networkPrefix>
116. show bgp vpnv6 unicast vrf <vrfName> <networkPrefix>/<subnetMask>
117. show bgp vpnv6 unicast vrf <vrfName> labels | include <networkPrefix>/<subnetMask>| [0-9A-Fa-f:;][0-9A-Fa-f]*
118. show bgp vpnv6 unicast summary | include BGP router identifier
119. show bgp vrf <vrfName> ipv6 unicast
120. show bgp vrf <vrfName> ipv6 unicast advertised neighbor <neighborId> summary | include <ceDeviceIpAddr>
121. show cef ipv6 summary
122. show cef vrf <vrfName> ipv6 <networkPrefix> detail
123. show cef vrf <vrfName> ipv6 <networkPrefix>/<subnetMask> detail
124. show cef vrf <vrfName> ipv6 <networkPrefix> location <location>
125. show cef vrf <vrfName> ipv6 <networkPrefix>/<subnetMask> location <location>
126. show ipv6 interface <interface>
127. show ipv6 interface brief <interface>
128. show ipv6 vrf all interface brief
129. show ipv6 vrf <vrfName> interface brief
130. show ipv6 vrf <vrfName> interface <interface>
131. show rib ipv6 tables
132. show route ipv6 <targetIp>
133. show route vrf <vrfName> ipv6 <targetIp>
134. show vrf <vrfName> ipv6 detail

