



CHAPTER 59

Using Cisco MPLS Diagnostics Expert

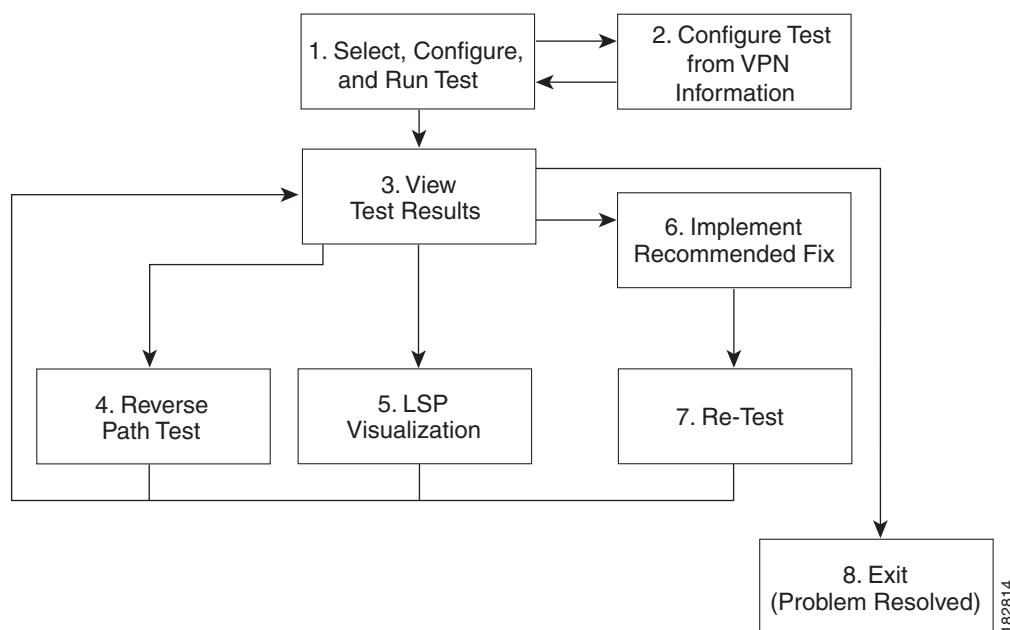
This chapter describes how to use Cisco Prime Diagnostics.

This chapter contains the following sections:

- [Understanding the Diagnostics Connectivity Tests, page 59-2](#)
- [Performing an MPLS VPN Connectivity Verification Test, page 59-6](#)
- [Progress Window, page 59-26](#)
- [Interpreting the Test Results, page 59-26](#)
- [Advanced Troubleshooting Options, page 59-32](#)
- [Switching Tunnel Checking Off—For Networks with Non-Cisco P Routers, page 59-35](#)

Figure 59-1 describes the workflow for using Prime Diagnostics.

Figure 59-1 **Using Diagnostics Workflow**



1. Select, Configure, and Run Test—Configure and run an MPLS VPN Connectivity Verification test. See [Performing an MPLS VPN Connectivity Verification Test, page 59-6](#).
2. Configure Test from VPN Information—Optionally configure an MPLS VPN Connectivity Verification test using VPN information. This is only possible if Prime Fulfillment VPN Provisioning functionality is used to provision VPNs within the network. See [Configuring Using Customer VRF Information, page 59-16](#) and [Configuring Using Customer VPN/VRF Information, page 59-18](#).
3. View Test Results—View results of MPLS VPN Connectivity Verification test, including the Test Log. See [Interpreting the Test Results, page 59-26](#).
4. Reverse Path Test—Perform Reverse Path Test advanced troubleshooting. See [Reverse Path Testing, page 59-33](#).
5. LSP Visualization—Perform LSP Visualization advanced troubleshooting. See [LSP Visualization, page 59-33](#).
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.

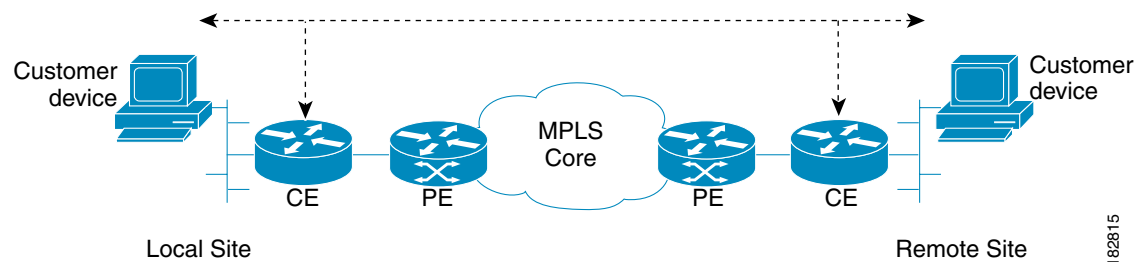
Understanding the Diagnostics Connectivity Tests

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 59-2](#)
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 59-3](#)
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 59-4](#)
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 59-4](#)
5. MPLS - PE to PE —Checks the MPLS Core connectivity between two PEs. See [L3VPN - PE to PE Connectivity Test, page 59-5](#)

L3VPN - CE to CE Connectivity Test

The L3VPN - CE to CE test ([Figure 59-2](#)) checks the MPLS VPN connectivity between two CEs or Customer devices where the Customer device IP address is known.

Figure 59-2 L3VPN - CE to CE Connectivity Test

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

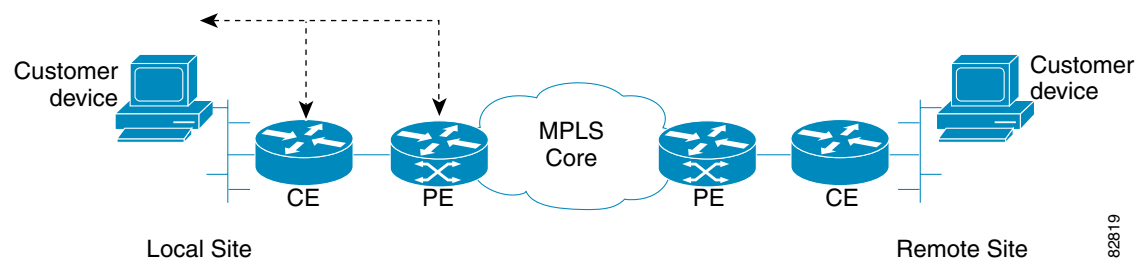
IPv6 troubleshooting

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 59-3) performs a VPN connectivity test between a PE and the locally attached CE. Diagnostics performs edge and attachment circuit troubleshooting in this case.

Figure 59-3 L3VPN - PE to Attached CE Connectivity Test

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

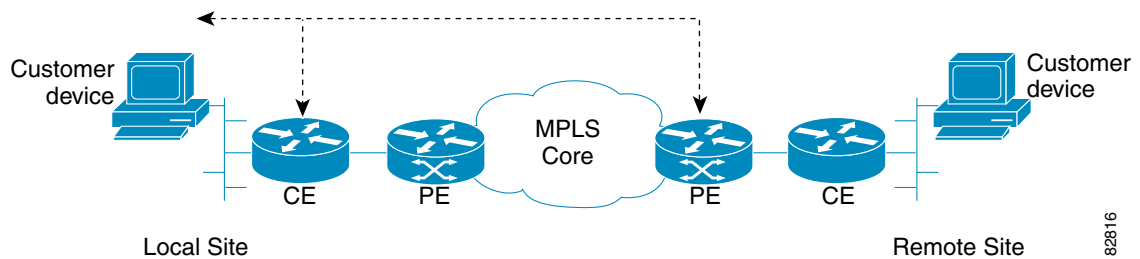
A L3VPN - PE to attached CE test launches troubleshooting on the IPv6 segment when all the following conditions are met:

- 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 59-4) 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 59-4 L3VPN - CE to PE Across Core Connectivity Test



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

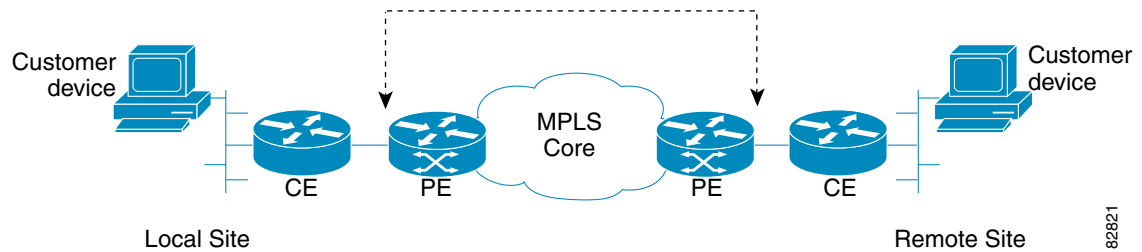
IPv6 troubleshooting

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 59-5) checks the MPLS VPN connectivity between two PEs. Diagnostics troubleshoots the core and the edge on both sides.

Figure 59-5 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.

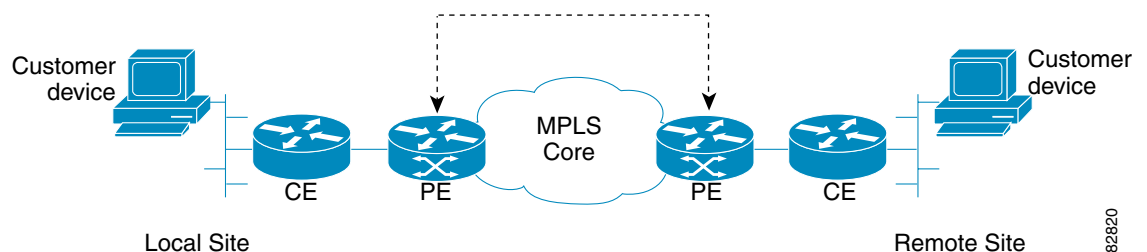
IPv6 troubleshooting

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 59-6](#)) checks the MPLS connectivity between two PEs.

Figure 59-6 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 59-6](#)
- [Selecting, Configuring, and Running a L3VPN - CE to CE Test, page 59-7](#)
- [Selecting, Configuring, and Running a L3VPN - PE to Attached CE Test, page 59-20](#)
- [Selecting, Configuring, and Running a L3VPN - CE to PE Across Core Test, page 59-21](#)
- [Selecting, Configuring, and Running a L3VPN - PE to PE Test, page 59-22](#)
- [Selecting, Configuring, and Running a MPLS - PE to PE Test, page 59-23](#)



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 Fulfillment. For details of how to log in, see the [Cisco Prime Fulfillment Installation Guide 6.1 \(Installing and Logging Into Prime Fulfillment > Logging In for the First Time\)](#).

The Prime Fulfillment 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 [Chapter 58, “User Roles”](#).

**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 [Chapter 58, “User Roles”](#) 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 59-2](#) 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 59-7 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

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.

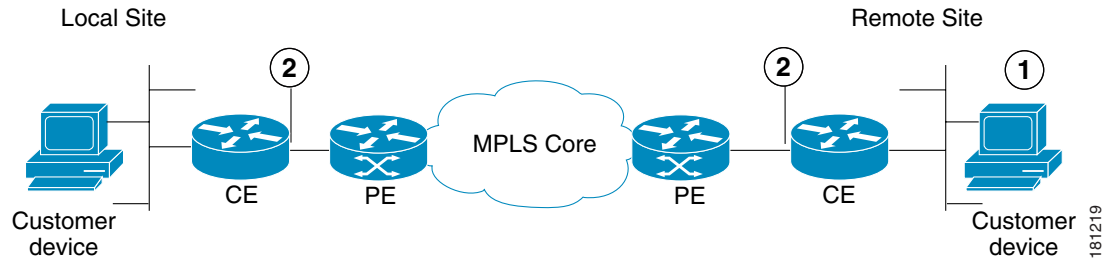
MPLS VPN Connectivity Verification tests connectivity between two sites in a VPN. Throughout the test, these sites are referred to as the local site and remote site. It is anticipated that a connectivity problem will be reported or detected from the perspective of a particular site. This particular site 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 59-8](#)) 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 59-8](#) as 1), or to the CE access circuit interface (shown in [Figure 59-8](#) 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 59-8 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 59-1](#) 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 59-18](#) for further information.

Table 59-1 *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 59-16.)
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 59-12).</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 59-1 **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 59-24 for further information.</p>
PE Access Circuit Interface	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 59-13).</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 Fulfillment device inventory.</p>

Table 59-1 *Field Descriptions for the L3VPN - CE to CE Diagnostics - Test Setup Window (continued)*

Field	Valid for Test Type	Description
CE Access CircuitInterface 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 59-18.)
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 59-26.](#)

Selecting a PE Device

Click the **Select** button (for the Local/Remote PE Device Name) to open the Select PE Device window (see [Figure 59-9](#)) 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 59-9](#). Possible values are Device Name, Provider, and PE Region Name.

Figure 59-9 **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 Fulfillment inventory, this overrides anything entered in the Local/Remote PE Device Name field (see [Figure 59-7](#).) 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 59-10](#)) 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 59-10 **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	ioxcgreen	VRF GREEN Link to MLS-1(CE3)
9	GigabitEthernet0/1/0/2.15	2001:db80:aace:1::1/64	ioxcgreen	VRF GREEN Link to MLS-1(CE3)
10	GigabitEthernet0/1/0/2.18	18.1.2.2/31	ioxcwhite	

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 Fulfillment inventory, this overrides anything entered in the Local/Remote PE Access Circuit Interface field (see [Figure 59-7](#)).

[Table 59-2](#) 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 59-10](#)). This saves large, time-consuming, and unnecessary searches which could occur in large networks. [Table 59-2](#) provides field descriptions for the Select Device Interface window.

Table 59-2 **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 59-21, and the [“Selecting, Configuring, and Running a L3VPN - PE to PE Test”](#) section on page 59-22 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 59-3](#) details the interface that must be entered in the PE Access Circuit Interface field for each multilink technology.

Table 59-3 **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 Fulfillment/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 Fulfillment Task Manager Collect Configuration task to upload the VRF names into Prime Fulfillment. 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 [Chapter 58, “Device Configuration Collection”](#).

- 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 59-4](#) 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 59-4](#) provides field descriptions for the Select Device for VRF Search window.

Table 59-4 *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 Fulfillment functionality. However, if Prime Fulfillment 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 Fulfillment 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 59-5](#) provides field descriptions for the Populate using VPN/VRF window.

Table 59-5 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 59-5 *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 59-26).

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 [Chapter 62, “VPN Topologies”](#) 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 59-3 for information on the PE to attached CE connectivity verification test type.

The MPLS VPN Connectivity Verification Configuration window appears ([Figure 59-11](#)) 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 59-11 L3VPN - PE to Attached CE Test Type

Test Representation

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

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:		

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 59-7.

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

[Table 59-1](#) on page 59-10 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 59-26.

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 59-4 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 59-12](#)) 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 59-12 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 59-7.

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

[Table 59-1](#) on page 59-10 provides descriptions of the fields applicable to the L3VPN - CE to PE across core test type.

2368659

- 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 59-26](#).

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 59-4](#) 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 59-13](#)) 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 59-13 L3VPN - PE to PE Test Type

L3VPN - 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 59-7](#).

- Step 2** Configure the fields in the L3VPN - PE to PE in VRF Diagnostics - Test Setup window as required. [Table 59-1 on page 59-10](#) 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 59-26](#).

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.

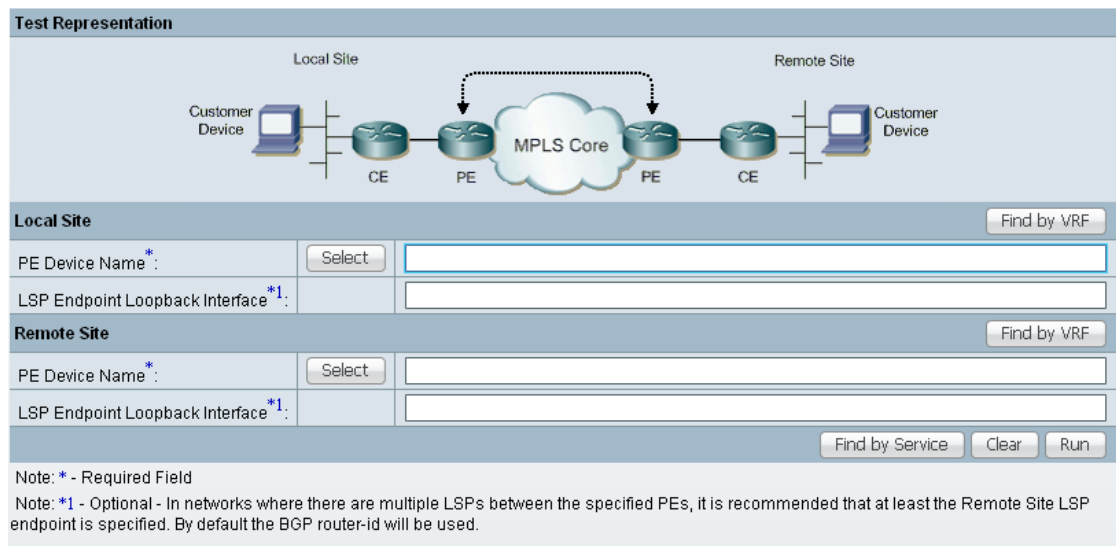
- Step 2** Click on the MPLS - PE to PE connectivity verification test type.

See the [“L3VPN - PE to PE Connectivity Test” section on page 59-5](#) for information on the PE to PE connectivity verification test type.

The MPLS - PE to PE window appears ([Figure 59-14](#)) 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 59-14 MPLS - PE to PE Test Type

MPLS - PE to PE



Test Representation

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

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 59-7](#).

238861

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

[Table 59-1 on page 59-10](#) 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 59-26](#).

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 59-15](#) 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.

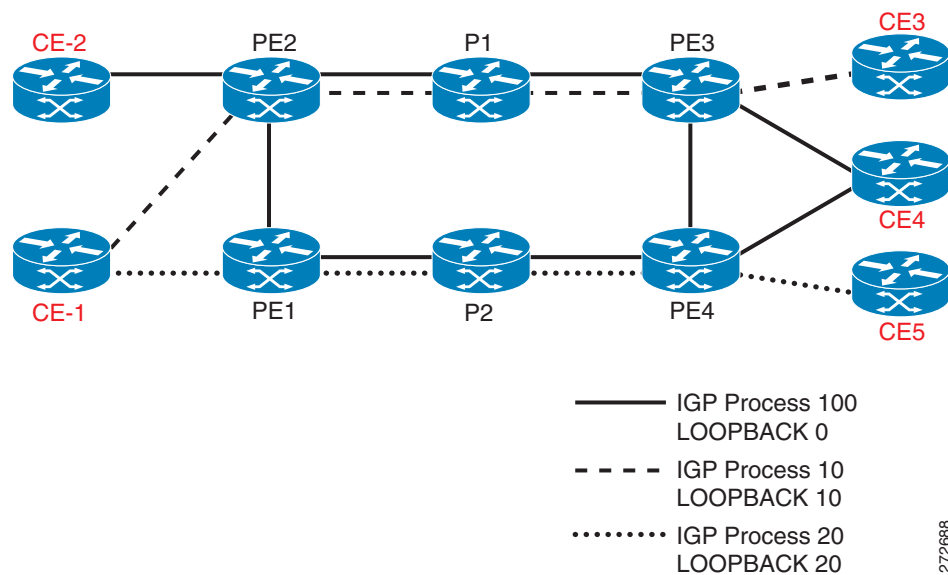
Figure 59-15 Example Network Topology

Table 59-6 provides IP addressing information relating to the example network topology displayed in Figure 59-15.

Table 59-6 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 59-7 specifies the IP addresses that can be used as the remote LSP Endpoint IP Address to test each LSP.

Table 59-7 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 59-16](#)) while the test is being performed.

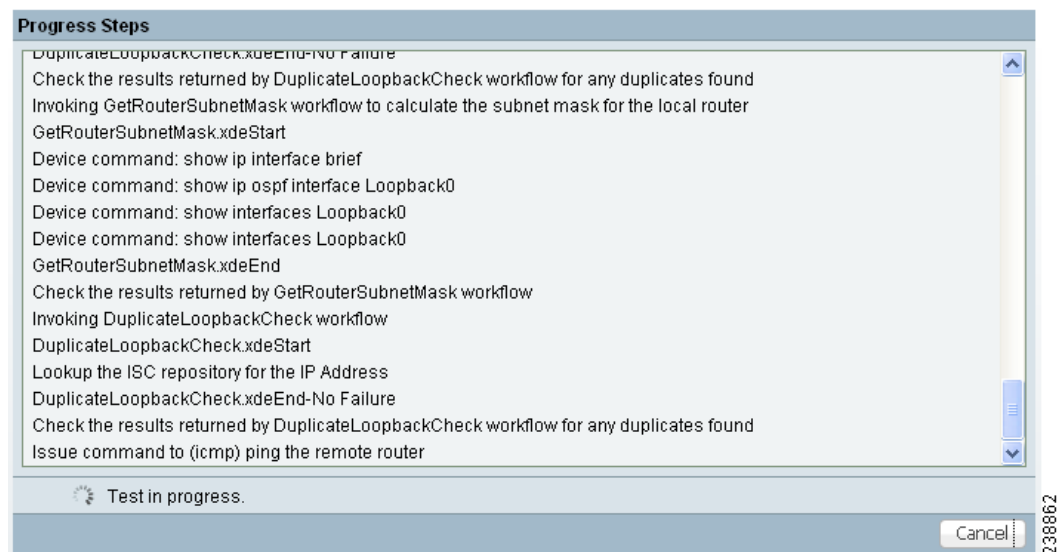


Note

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 59-16 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 59-26, 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 59-28](#)
- [Test Details, page 59-30](#)
- [Test Log, page 59-31](#)
- [Export, page 59-32](#)

Upon completion of a MPLS VPN Connectivity Verification test, the Test Results window appears (see [Figure 59-17](#)).

Figure 59-17 Test Results Window with Failure Specific Additional Information Displayed

Test Representation

CE 192.168.1.10 GigE1/7 cl-test-core-12404-1 PE -/20 GigE1/0 cl-test-core-7304-1 P 20/17 GigE1 cl-test-core-7204-1 P 17/16 FE2/0 cl-test-core-7204-1 P 16/No Label FE0/0 cl-test-core-7507-1 PE -/ FE4/0 cl-test-core-7206-3 CE 192.168.1.10

Result

View: ☒ Test Details ☐ Test Log

Summary: 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.

Possible Cause(s): CEF not enabled on router cl-test-core-7206-3.

Recommended Action: Enable CEF on router cl-test-core-7206-3.

Device: cl-test-core-12404-1

Command: show interfaces POS3/3

```
POS3/3 is administratively down, line protocol is down
Hardware is Packet over SONET
MTU 4470 bytes, BW 155000 Kbit, DLY 100 usec, rely 255/255, load 1/255
Encapsulation HDLC, crc 16, loopback not set
Keepalive set (10 sec)
Scramble disabled
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Available Bandwidth 149259 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 parity
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 applique, 0 interface resets
  0 output buffer failures, 0 output buffers swapped out
  0 carrier transitions
```

Advanced Re-test Cancel

The Test Result window displays the location and cause of the problem found, recommended actions, observations, and details of the automated troubleshooting and diagnostics steps performed. The Test Result window also allows you to invoke advanced troubleshooting options where appropriate (see [Table 59-8](#)).

The Test Results window consists of the following components:

Table 59-8 Field Descriptions for the Test Results Window

Field/Button	Description
Data path	See the “Data Path” section on page 59-28
Test Details	See the “Test Details” section on page 59-30
Test Log	See the “Test Log” section on page 59-31
Export button	The Export button appears when the Test Log radio button is selected. See the “Export” section on page 59-32.
Advanced button	Click the Advanced button to launch advanced troubleshooting. See the “Advanced Troubleshooting Options” section on page 59-32. The options available on this button are dynamically configured depending on the test result and the test type.

Table 59-8 *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.

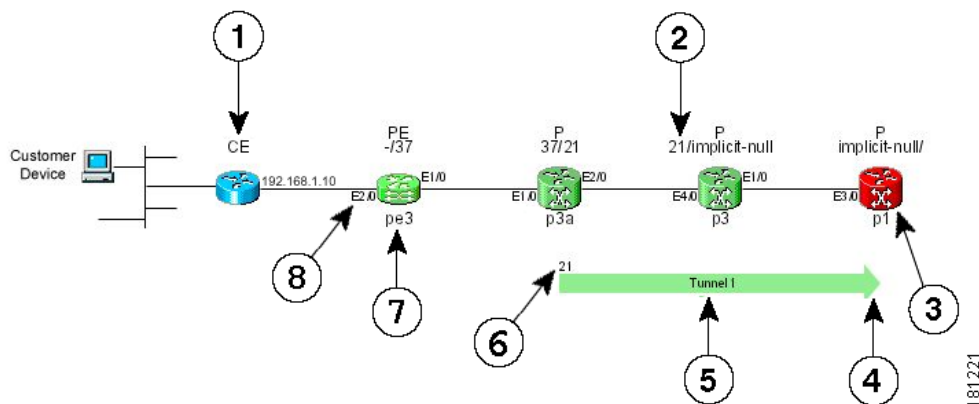
The other test types troubleshoot in the same order, but do not perform all of the steps.

**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 59-18](#)) 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 59-18 *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 59-9](#).

Table 59-9 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 59-10](#).

Table 59-10 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 59-17 on page 59-27](#)) displays a summary of the automated troubleshooting and diagnostics results, observations made during troubleshooting, additional failure-specific information, and recommended action. See [Chapter 63, “Failure Scenarios”](#) 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 59-17 on page 59-27](#) 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 59-19](#) 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 59-19 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 59-20) radio button to display details of all troubleshooting and diagnostics steps in the order in which they were performed.

Figure 59-20 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.

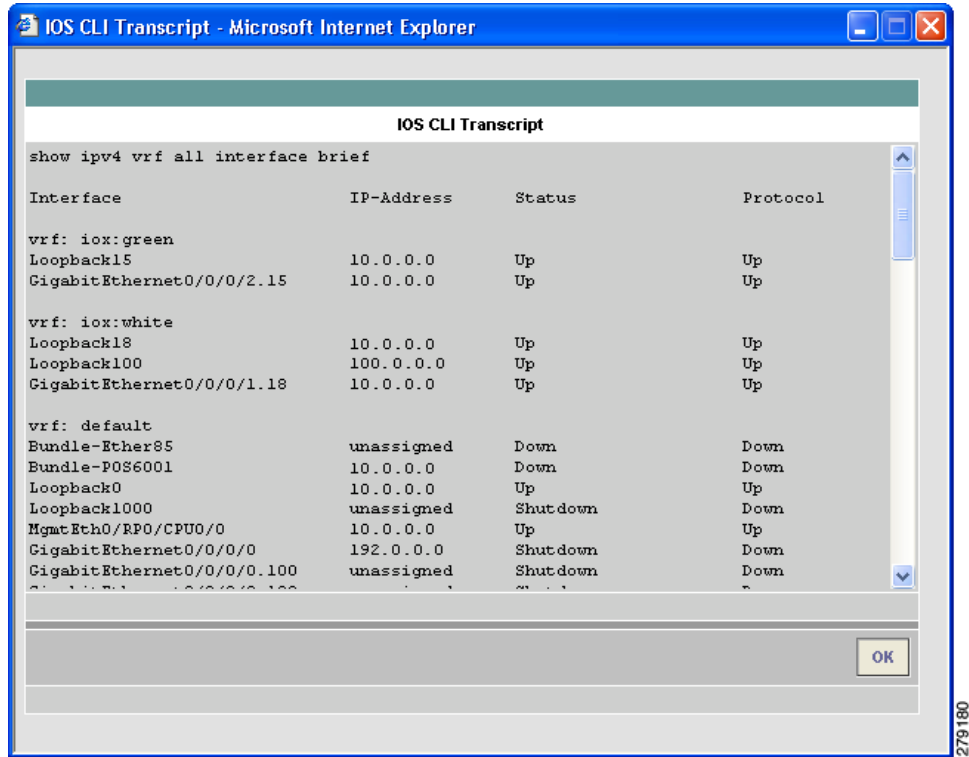
Warning: No LSP Endpoint Loopback IP Address was specified for the remote site host cl-test-ac-7200-10. The BGP router-id of the remote site host was used as the LSP endpoint for LSP troubleshooting. This may result in the incorrect LSP being tested.

Advanced Re-test Cancel

238861

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 59-21](#)). This transcript includes the IOS or IOS XR commands run and all resulting output.

Figure 59-21 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 59-20 on page 59-31](#)). 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 59-33](#)
- [LSP Visualization, page 59-33](#)

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

The advanced troubleshooting options supported are detailed in [Table 59-11](#).

Table 59-11 **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



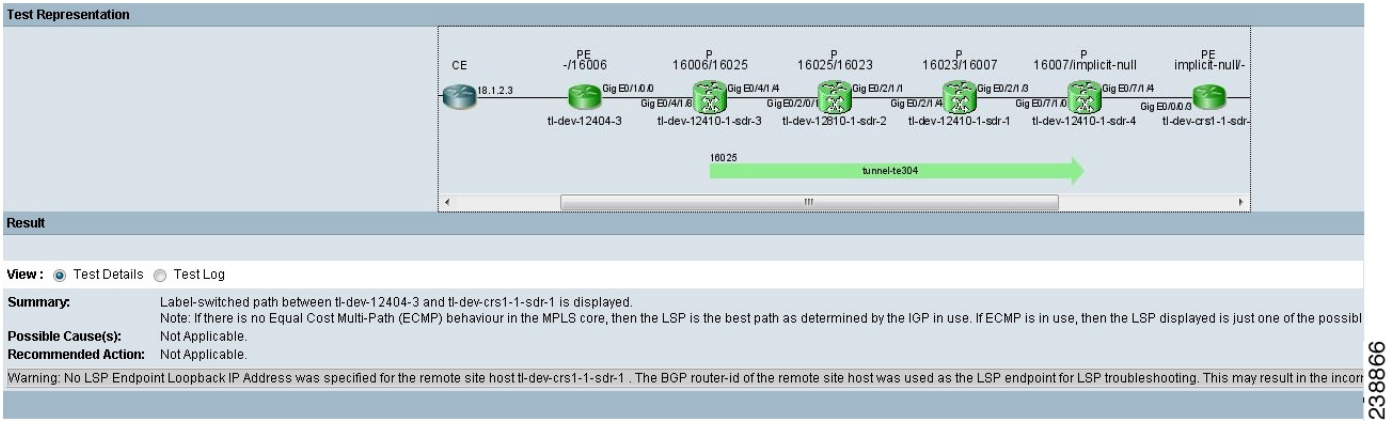
Note

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 59-22). 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 59-22 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

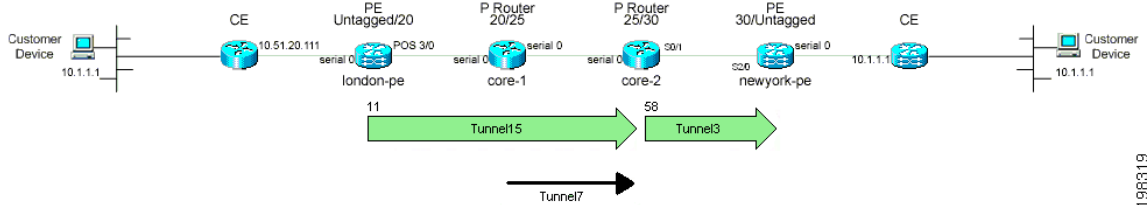


Note

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 59-23 Multiple MPLS TE Tunnel Configuration



For more details of what is displayed in the Data Path, see the [“Data Path” section on page 59-28](#).

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 Fulfillment 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.

