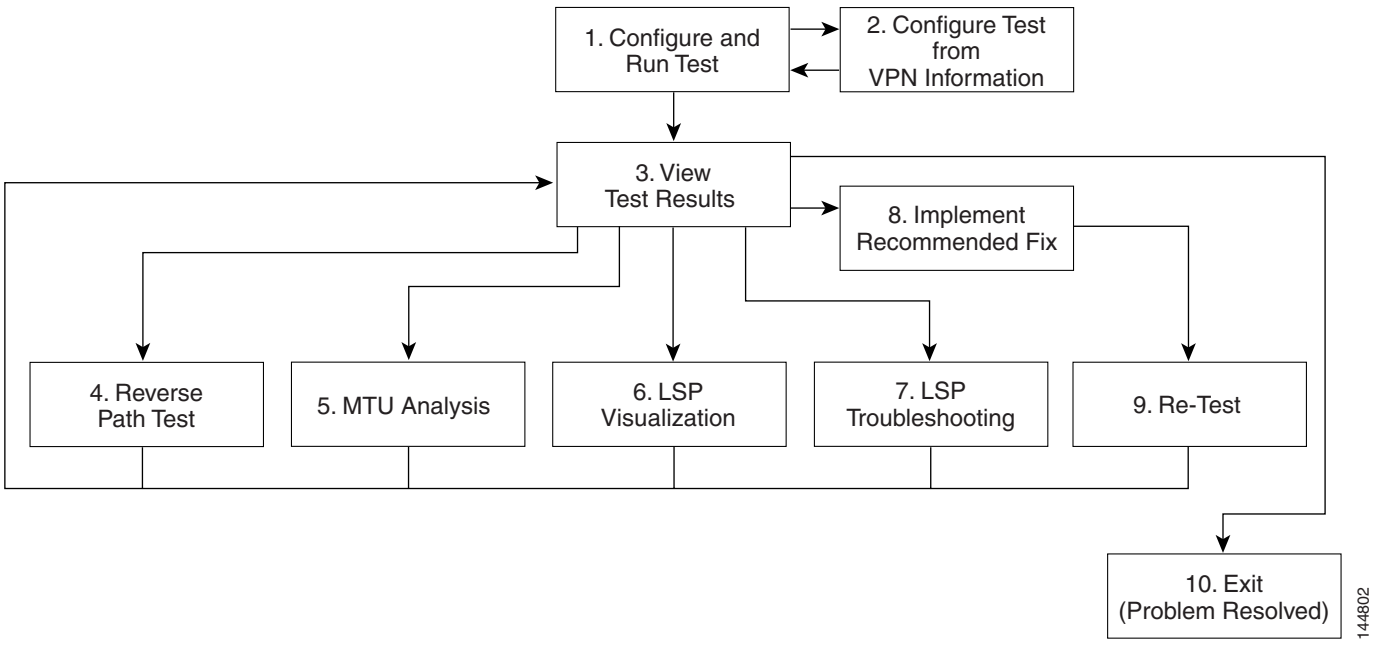
Using Cisco MPLS Diagnostics Expert

This chapter describes how to use Cisco MPLS Diagnostics Expert.

This chapter contains the following sections:

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

Figure 3-1 Using Cisco MPLS Diagnostics Expert Workflow



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

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

3.1 Performing an MPLS VPN Connectivity Verification Test

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

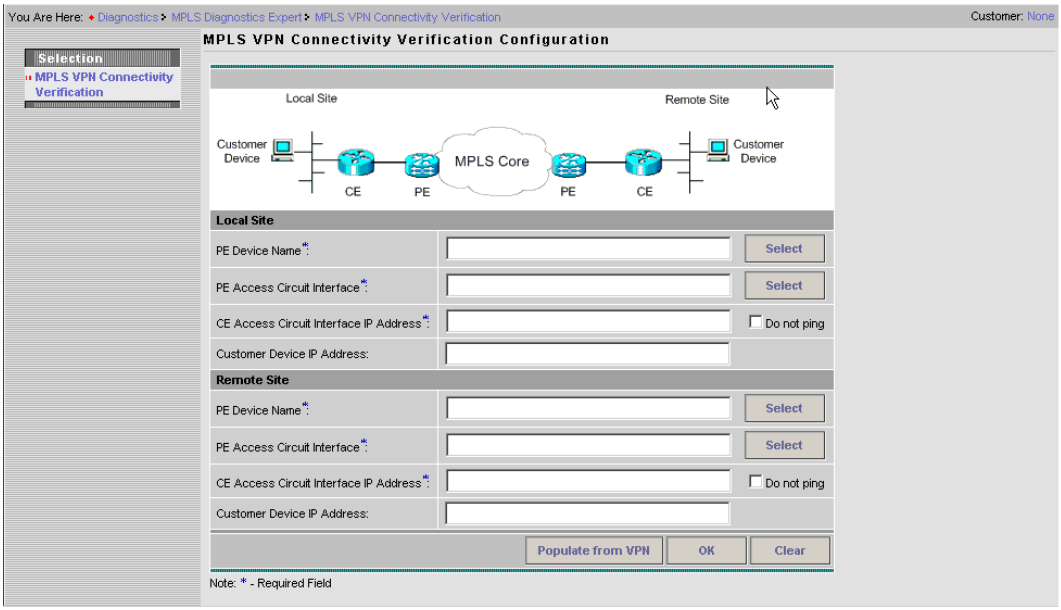
Note When performing parallel MPLS VPN Connectivity Verification tests on the same client machine, ensure each test is performed using a different HTTP session. To do so, run each test in a separate browser, launched from the command line, or by clicking on the browser icon on the desktop, or Start menu.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

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

Figure 3-2 Diagnostics Tab

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

Figure 3-3 MPLS VPN Connectivity Verification Configuration Window



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

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

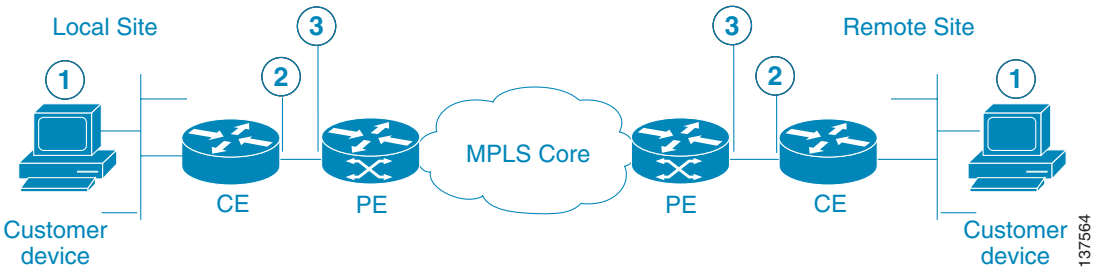
The network diagram is a static image that provides you with context for the information you must enter to configure the test.

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

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

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

Figure 3-4 Test Scope



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

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

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

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

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

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

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

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

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

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

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

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

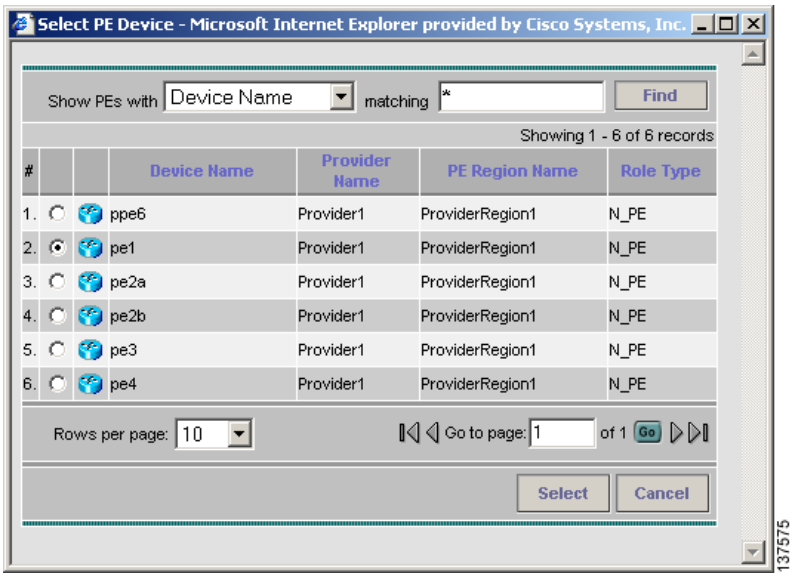
Table 3-1 Field Descriptions for the MPLS VPN Connectivity Verification Configuration Window (continued)

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

Selecting a PE Device

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

Figure 3-5 Select PE Device Window



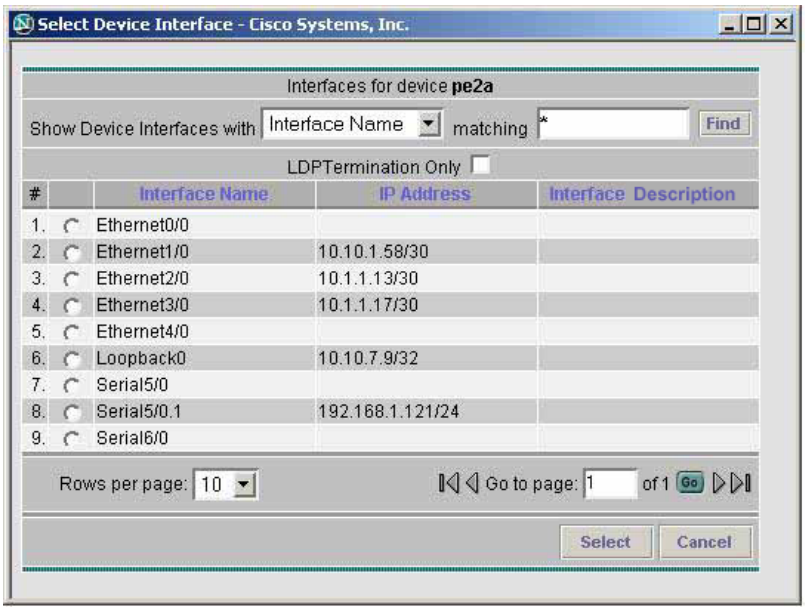
You can perform a wildcard string search of all PE attributes displayed in the PE table. If you select a local/remote site PE from the ISC inventory, this overrides anything entered in the Local/Remote PE Device Name field (see Figure 3-3.)

Selecting a PE Access Circuit Interface

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

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

Figure 3-6 Select Device Interface Window



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

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

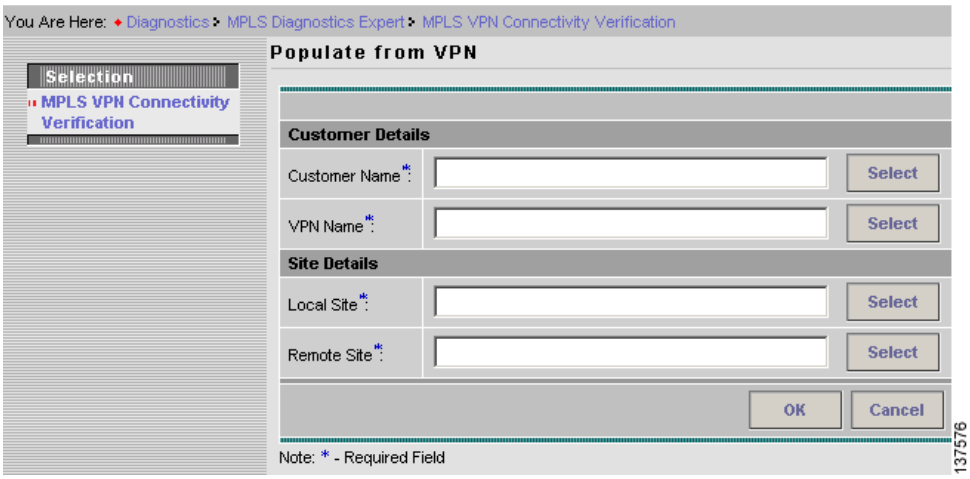
3.1.1 Configuration Using Customer VPN Information

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

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

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

Figure 3-7 Populate from VPN Window



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

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

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

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

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

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

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

3.1.2 VPN Topologies

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

3.1.2.1 Testing with Hub and Spoke VPN Topology

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

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

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

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

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

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

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

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

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

Figure 3-8 Workflow

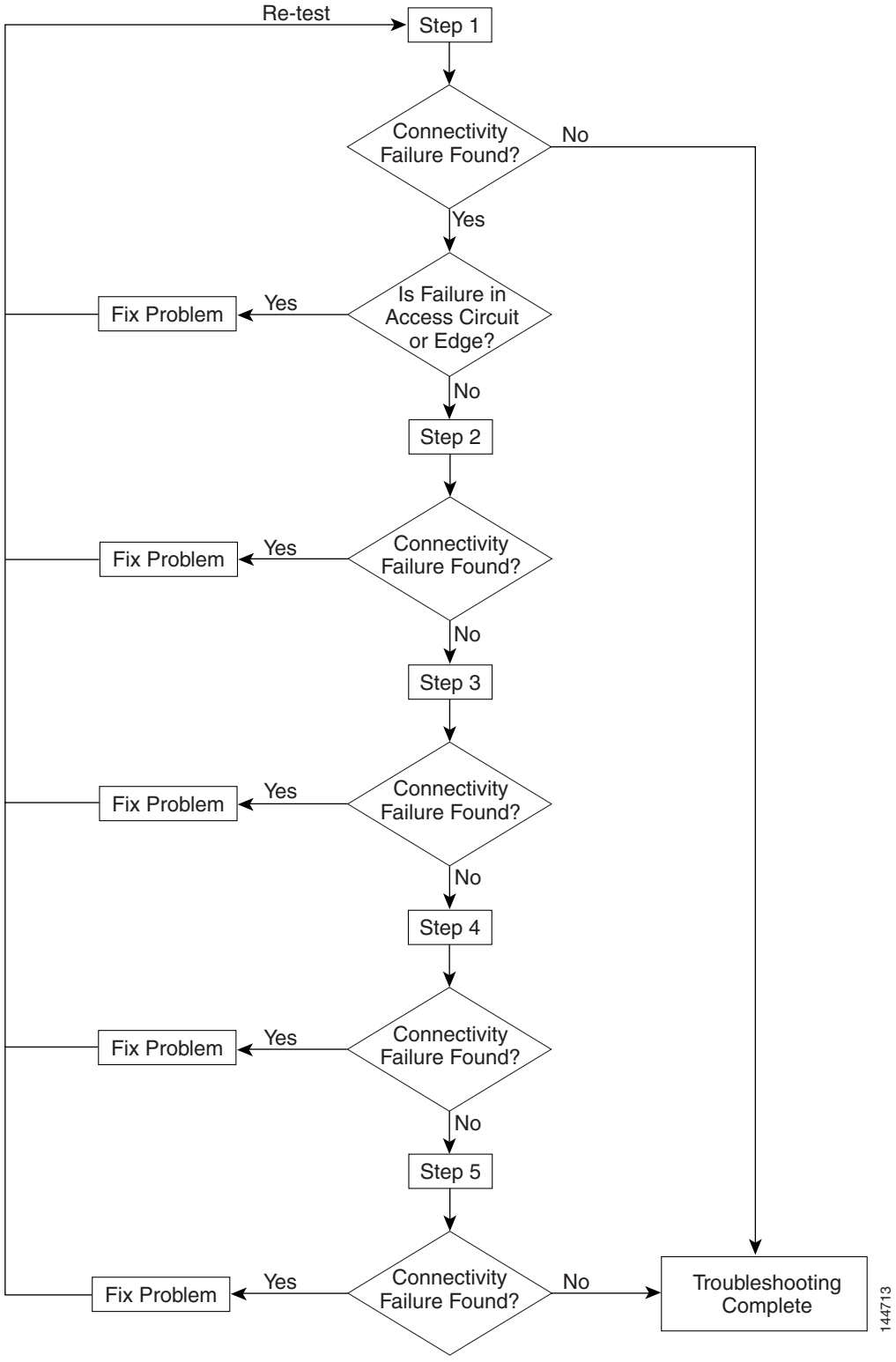
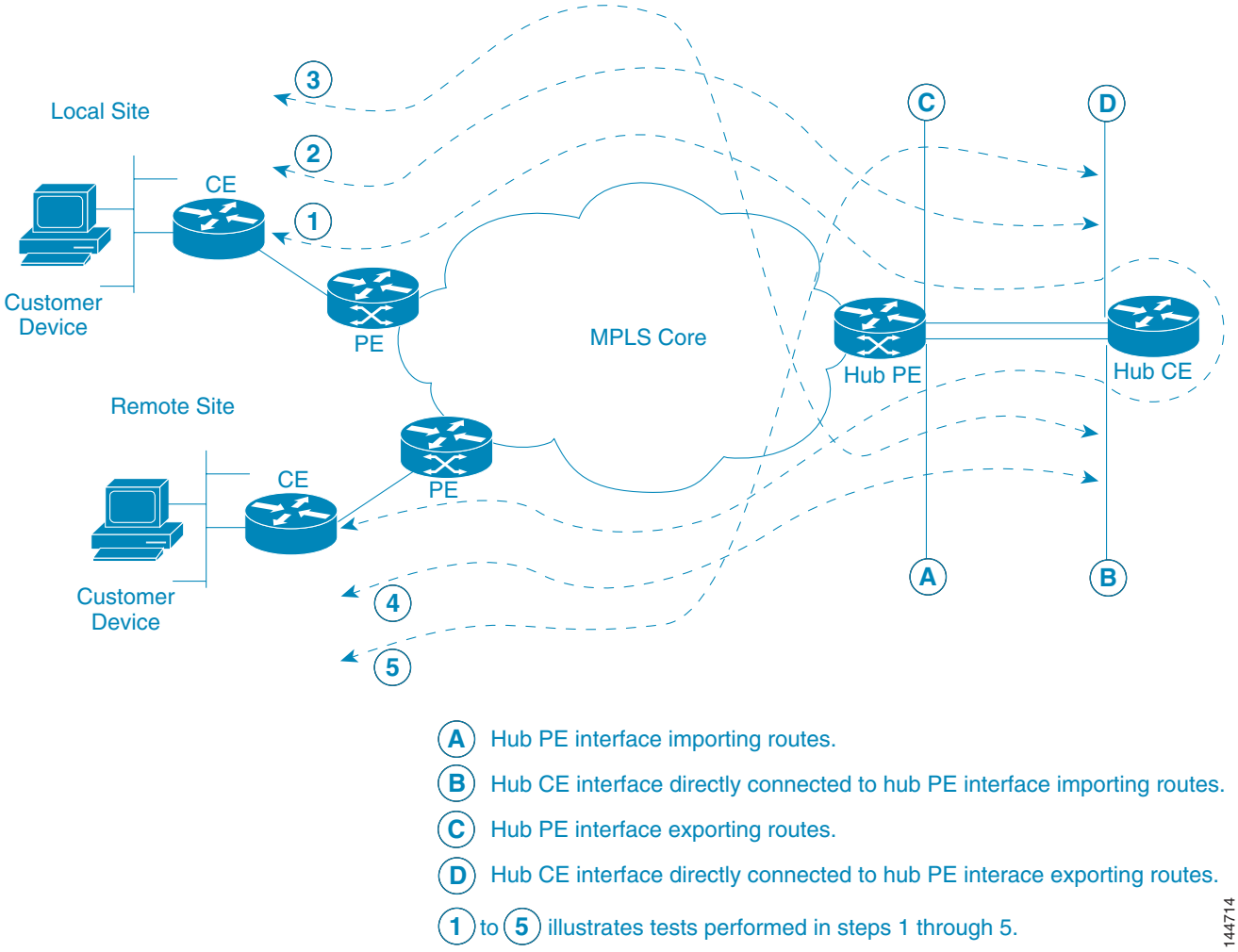


Figure 3-9 illustrates the MPLS VPN Connectivity Verification tests required to test connectivity between two sites in a hub and spoke VPN.

Figure 3-9 Testing a Hub and Spoke VPN Topology



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

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

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

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

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

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

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

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

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

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

3.1.2.2 Testing with Intranet/Extranet VPN Topology

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

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

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

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

3.1.2.3 Testing with Central Services VPN Topology

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

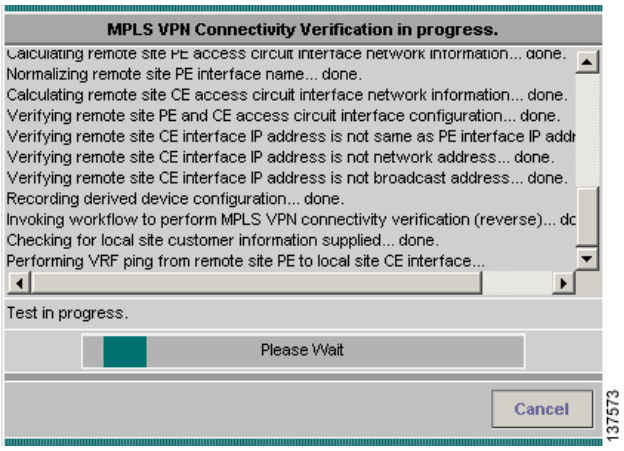
It is not possible to perform an MPLS VPN Connectivity Verification test between two client sites in a Central Services VPN.

3.1.3 Progress Window

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

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

Figure 3-10 Progress Window



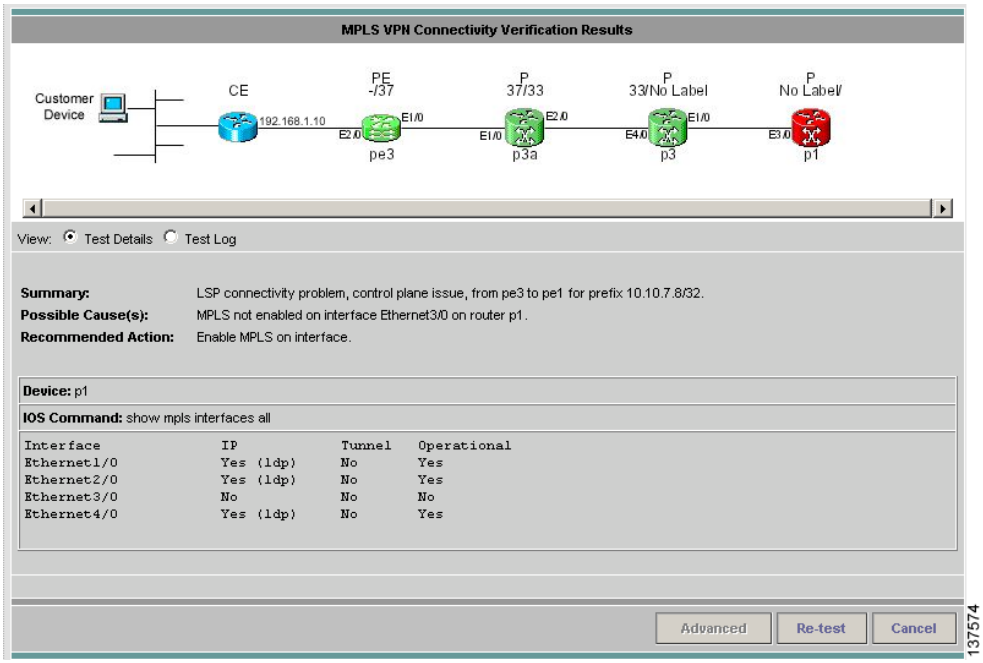
Click the Cancel button to cancel the test if required. If you click **Cancel**, you are asked to confirm that you want to cancel the test. If you confirm, the test is cancelled when the current step has completed. If the current step involves device interaction, this completes before the test is cancelled.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

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

3.2 Interpreting the Test Results

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

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



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

The Test Results window consists of the following components:

Table 3-5 Field Descriptions for the Test Results Window

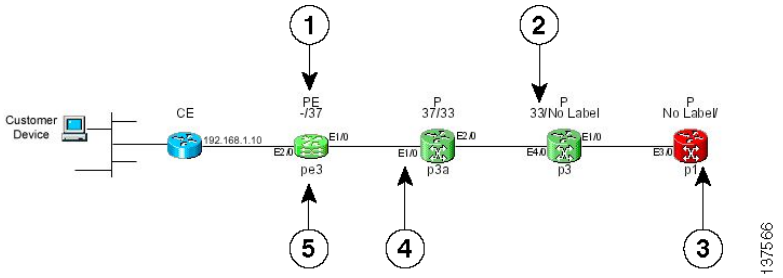
Field/Button	Description
Data path	See 3.2.1 Data Path, page 3-17
Test Details	See 3.2.2 Test Details, page 3-19
Test Log	See 3.2.3 Test Log, page 3-21
Export button	The Export button appears when the Test Log radio button is selected. See 3.2.4 Export, page 3-22.
Advanced button	Click the Advanced button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

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

3.2.1 Data Path

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

Figure 3-12 Data Path



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

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

Table 3-6 Data Path Device Color Codes

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

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

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

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

Table 3-7 Data Path Link Color Code

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

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

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

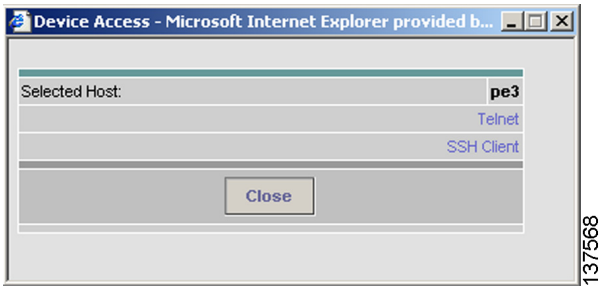
The information displayed for CE devices and customer devices is minimal. Typically only the information provided during test configuration is displayed for these devices.

3.2.1.1 Device Actions

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

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

Figure 3-13 Device Actions



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

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

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

3.2.2 Test Details

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

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

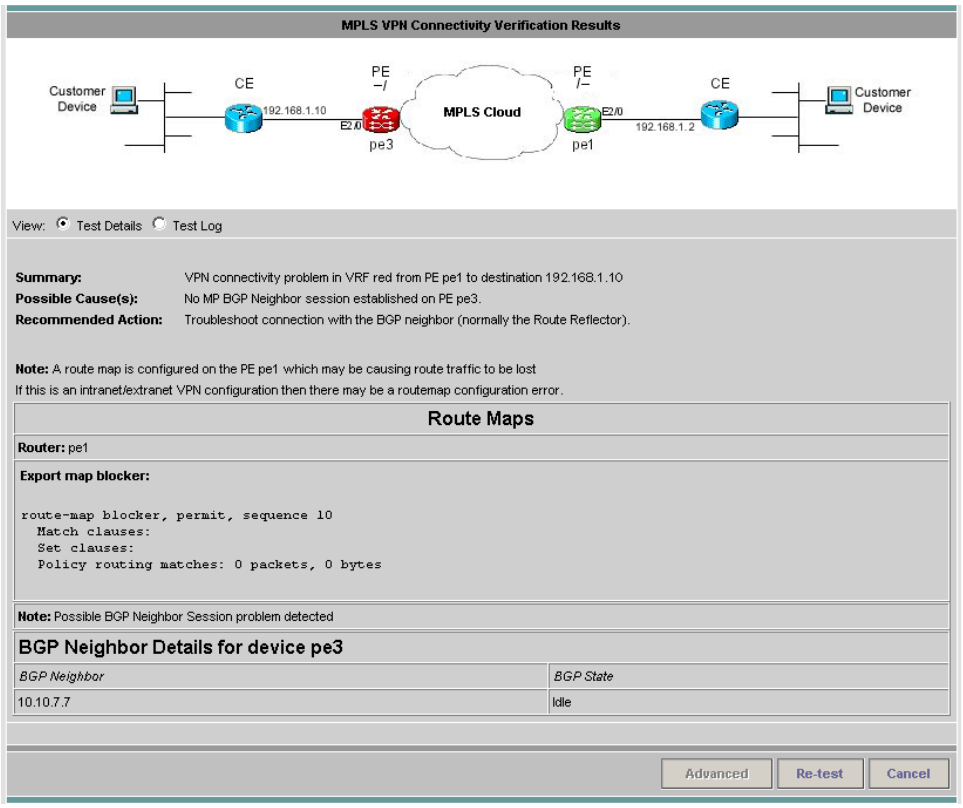
- Summary—Displays a brief summary of the failure found.
- Possible Cause(s)—Possible causes of the failure.
- Recommended Action—Recommended actions to resolve the problem.

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

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

The Test Details radio button is selected by default.

Figure 3-14 Test Results Window with Observation Notes

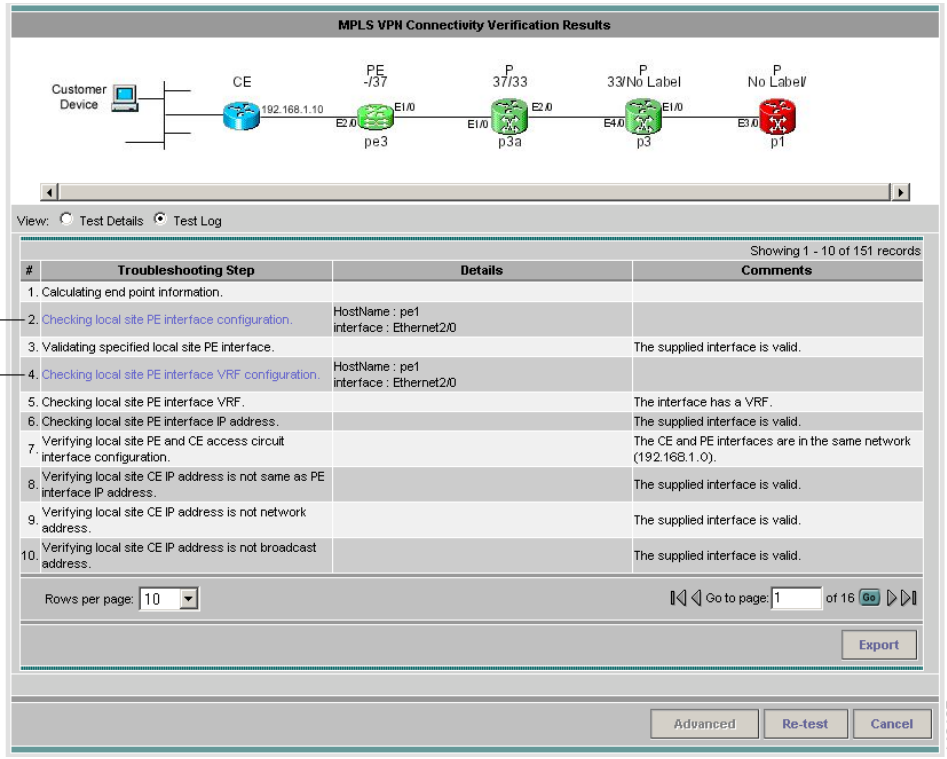


Observations made during troubleshooting are displayed as notes below the Test Details summary. Observation notes detail observations made during troubleshooting which could be related to the failure. They should be considered as additional troubleshooting information. Figure 3-14 shows an example Test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

3.2.3 Test Log

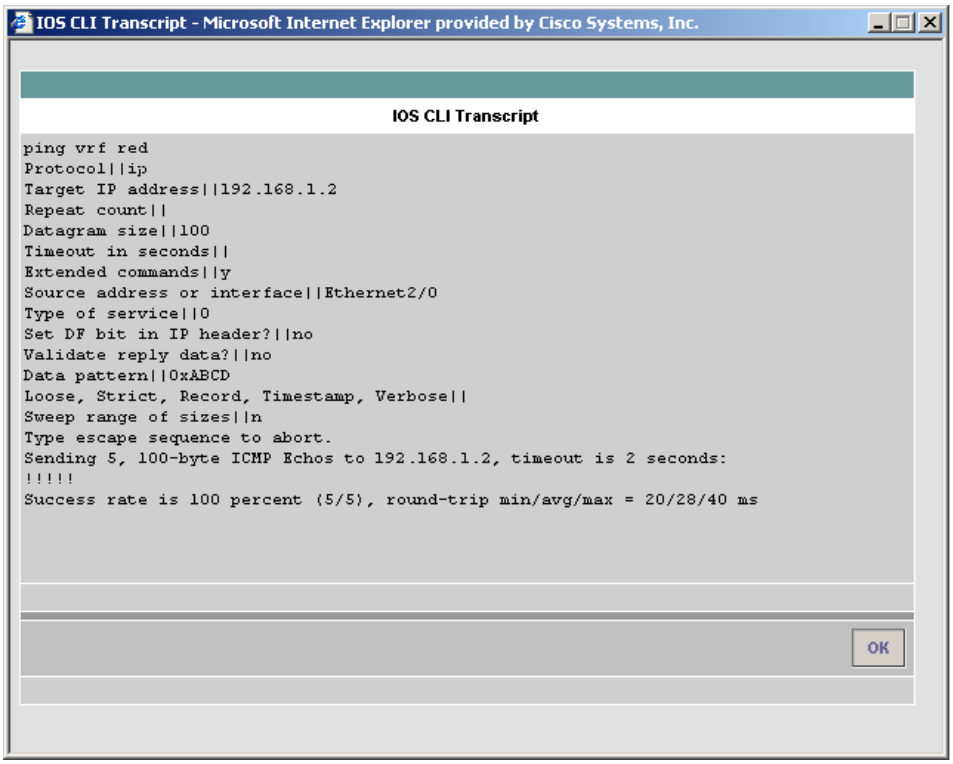
Click the Test Log (see Figure 3-15) radio button to display details of all troubleshooting and diagnostics steps in the order in which they were performed.

Figure 3-15 Test Results Window—Test Log



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

Figure 3-16 IOS CLI Transcript Window



3.2.4 Export

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

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

Step 2 Save the file.

3.3 Advanced Troubleshooting Options

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

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

Table 3-8 Advanced Troubleshooting Options

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

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

3.3.1 Reverse Path Testing

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

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

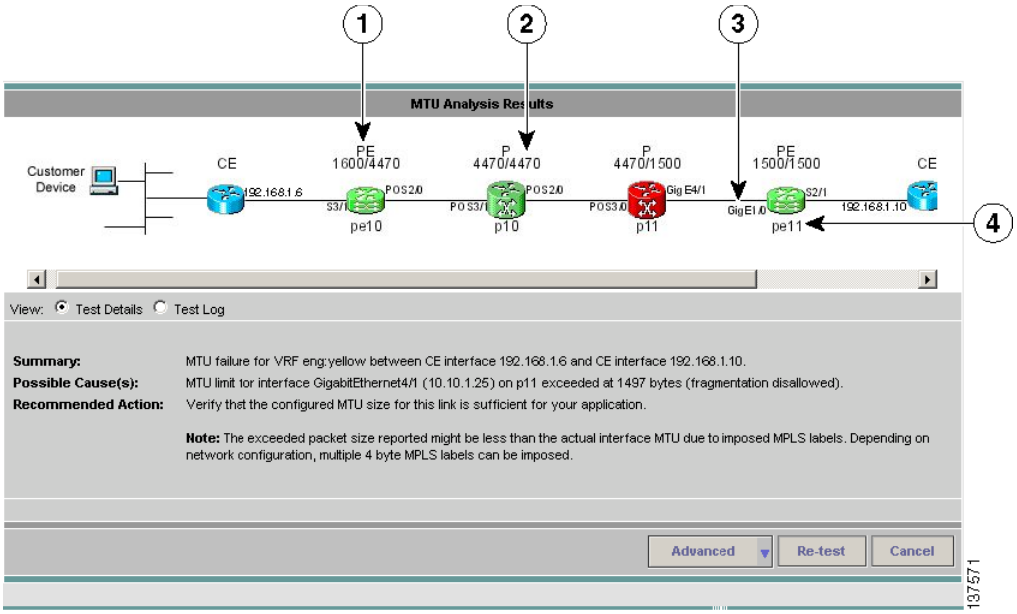
The results of the reverse path testing are displayed in the Test Results window.

3.3.2 MTU Analysis

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

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

Figure 3-17 Test Results Window—MTU Analysis Results



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

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

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

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

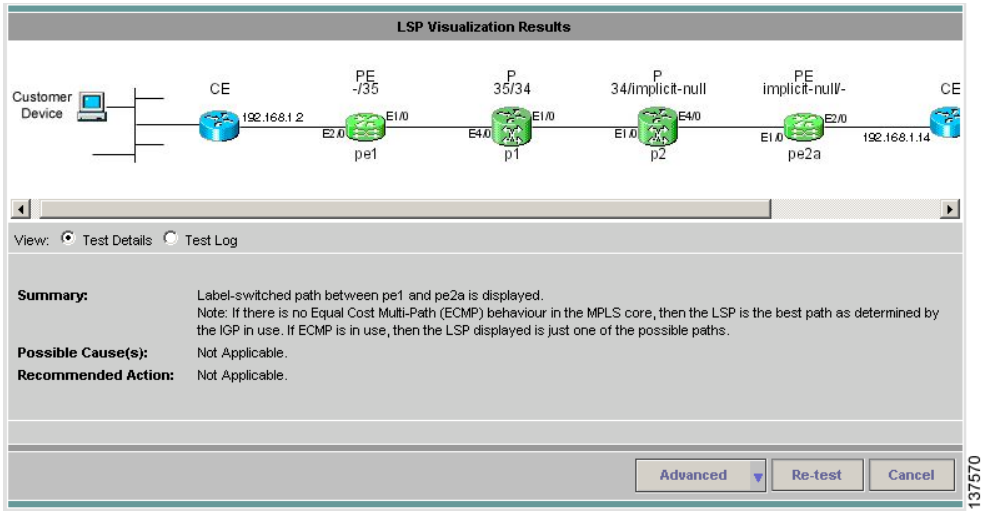
MTU analysis is only offered when an MPLS VPN Connectivity Verification test does not detect a connectivity problem.

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

3.3.3 LSP Visualization

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

Figure 3-18 Test Results Window—LSP Visualization



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

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

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

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

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

3.3.4 LSP Troubleshooting

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