CHAPTER 62

VPN Topologies

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

Testing with Full Mesh VPN Topology

By default, an MPLS VPN Connectivity Verification test assumes that the local and remote sites are connected through a full mesh VPN topology and that these sites can communicate directly. For details of how to configure an MPLS VPN Connectivity Verification test for a full mesh VPN topology, see Chapter 59, “Performing an MPLS VPN Connectivity Verification Test”.

Testing with Hub and Spoke VPN Topology

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

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

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

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

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

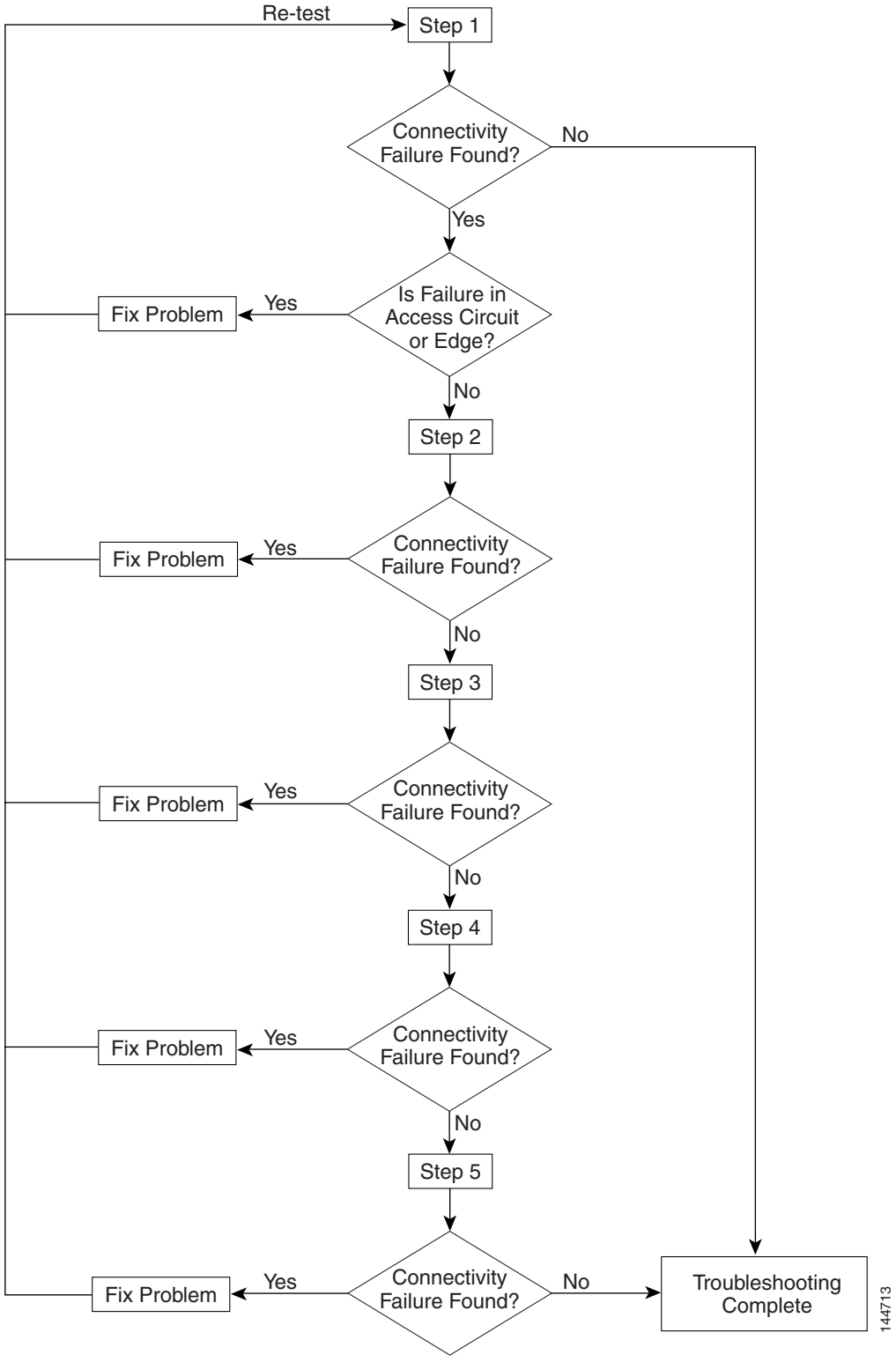
Step 5 MPLS VPN Connectivity Verification test between the remote site and the hub CE interface that is attached to the hub PE interface exporting routes.

Each step involves performing an MPLS VPN Connectivity Verification test between different points. Depending on whether a connectivity failure exists and the location of this failure, it might not be necessary to perform all five steps. Figure 62-1 shows the workflow for testing a hub and spoke VPN.

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

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

Figure 62-1 Workflow

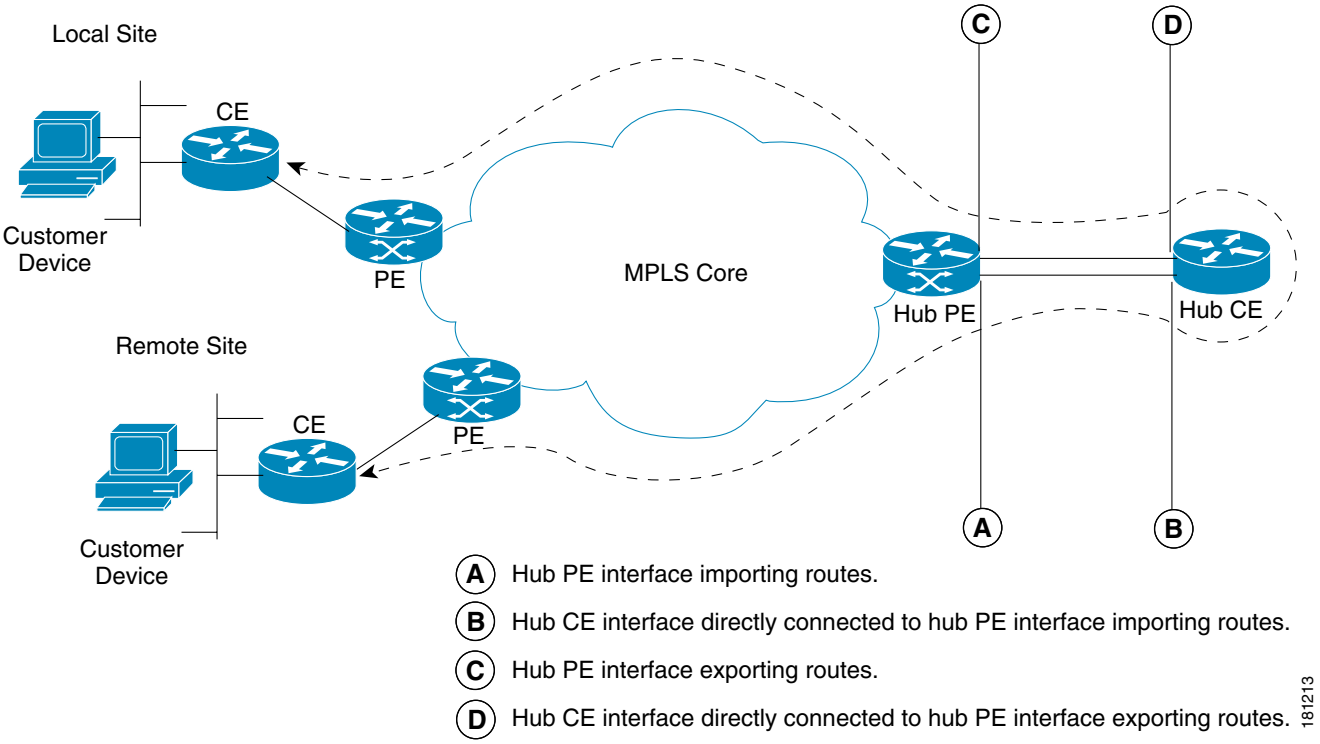


1. You should perform an MPLS VPN Connectivity Verification test between the local and remote sites. If this test finds no connectivity problems, then no further troubleshooting is required. If this test reports a connectivity failure caused by an MPLS problem, you should ignore the test result and move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

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

Figure 62-2 illustrates the MPLS VPN Connectivity Verification tests required to test connectivity between two sites in a hub and spoke VPN.

Figure 62-2 Testing a Hub and Spoke VPN Topology—Step 1

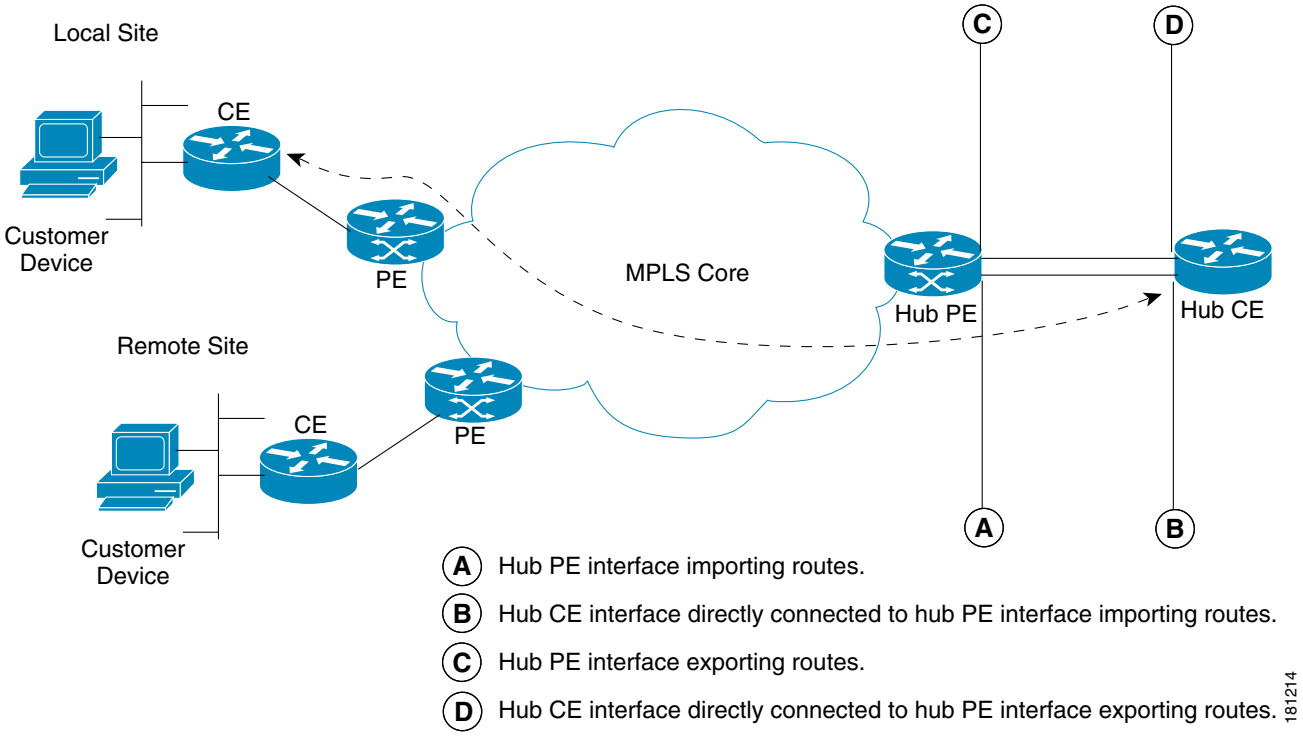


2. You should perform an MPLS VPN Connectivity Verification test between the local site (Spoke) and the hub CE interface that is attached to the hub PE interface which imports routes (shown in Figure 62-3 as *B*). When configuring the MPLS VPN Connectivity Verification test, the Local Site fields on the MPLS VPN Connectivity Verification Configuration window should be configured with details of the local customer site. The Remote Site fields should be configured with details of the Hub PE/CE interfaces that import routes (shown in Figure 62-3 as *A* and *B*), as shown in Table 62-1.

Table 62-1 Test Configuration—Hub Route Import Interface Tests

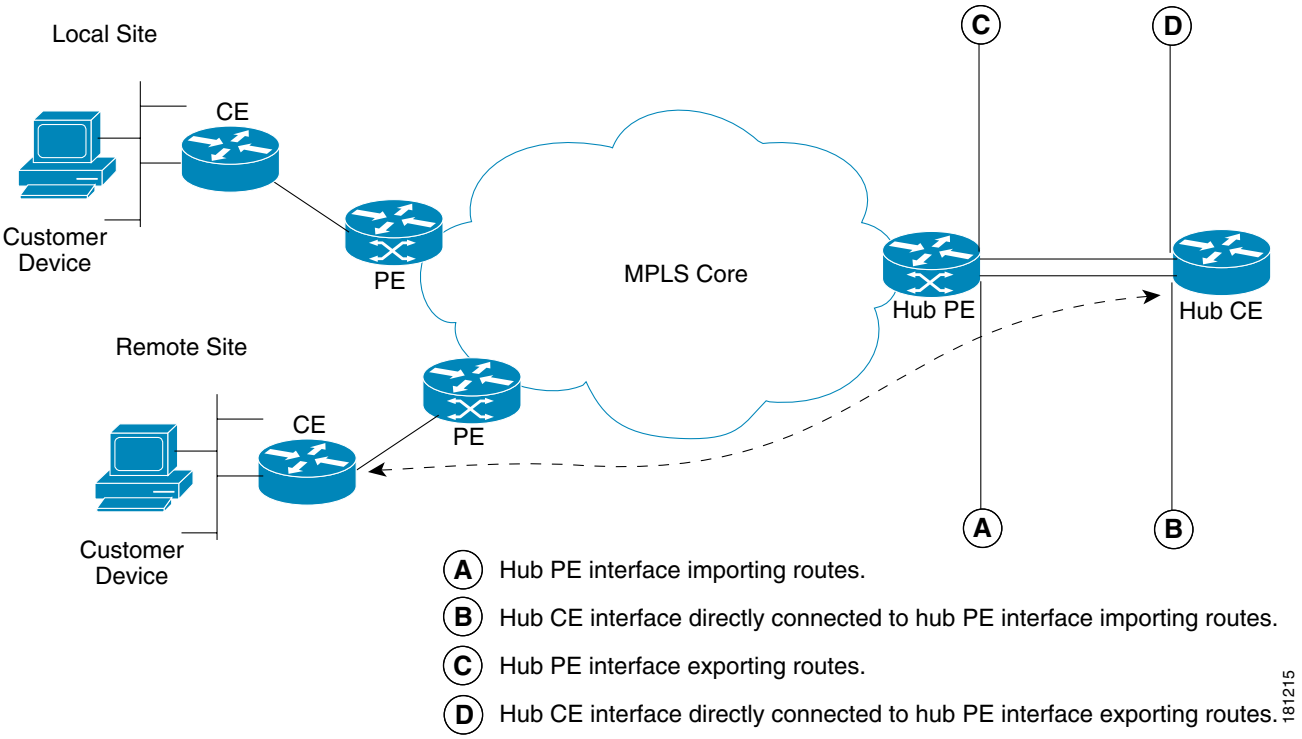
Field Name	Hub Detail
PE Device Name	Hub PE device name.
PE Access Circuit Interface	Hub PE interface which imports routes.
CE Access Circuit Interface IP Address	IP address of hub CE interface directly connected to PE interface which imports routes.
Customer Device IP Address	Leave blank.

Figure 62-3 Testing a Hub and Spoke VPN Topology—Step 2



3. You should perform an MPLS VPN Connectivity Verification test between the remote site (Spoke) and the hub CE interface that is attached to the hub PE interface which imports routes (shown in Figure 62-4 as *B*). When configuring the MPLS VPN Connectivity Verification test, the Local Site fields should be configured with details of the Hub PE/CE interfaces that import routes (shown in Figure 62-4 as *A* and *B*), as shown in Table 62-1. The Remote Site fields on the MPLS VPN Connectivity Verification Configuration window should be configured with details of the remote customer site.

Figure 62-4 Testing a Hub and Spoke VPN Topology—Step 3

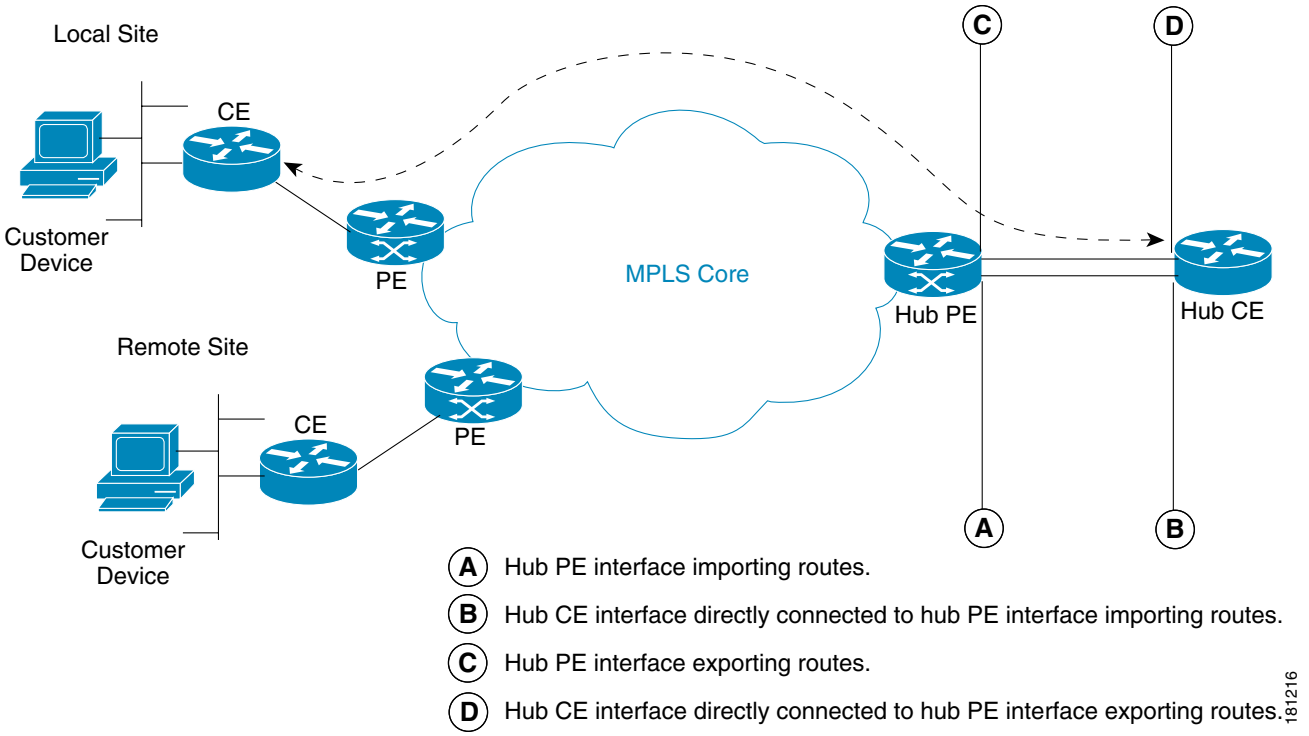


4. You should perform an MPLS VPN Connectivity Verification test between the local site (Spoke) and the hub CE interface that is attached to the hub PE interface which exports routes (shown in Figure 62-5 as *D*). When configuring the MPLS VPN Connectivity Verification test, the Local Site fields on the MPLS VPN Connectivity Verification Configuration window should be configured with details of the local customer site. The Remote Site fields should be configured with details of the Hub PE/CE interfaces that export routes (shown in Figure 62-5 as *C* and *D*), as shown in Table 62-2.

Table 62-2 Test Configuration —Hub Route Export Interface Tests

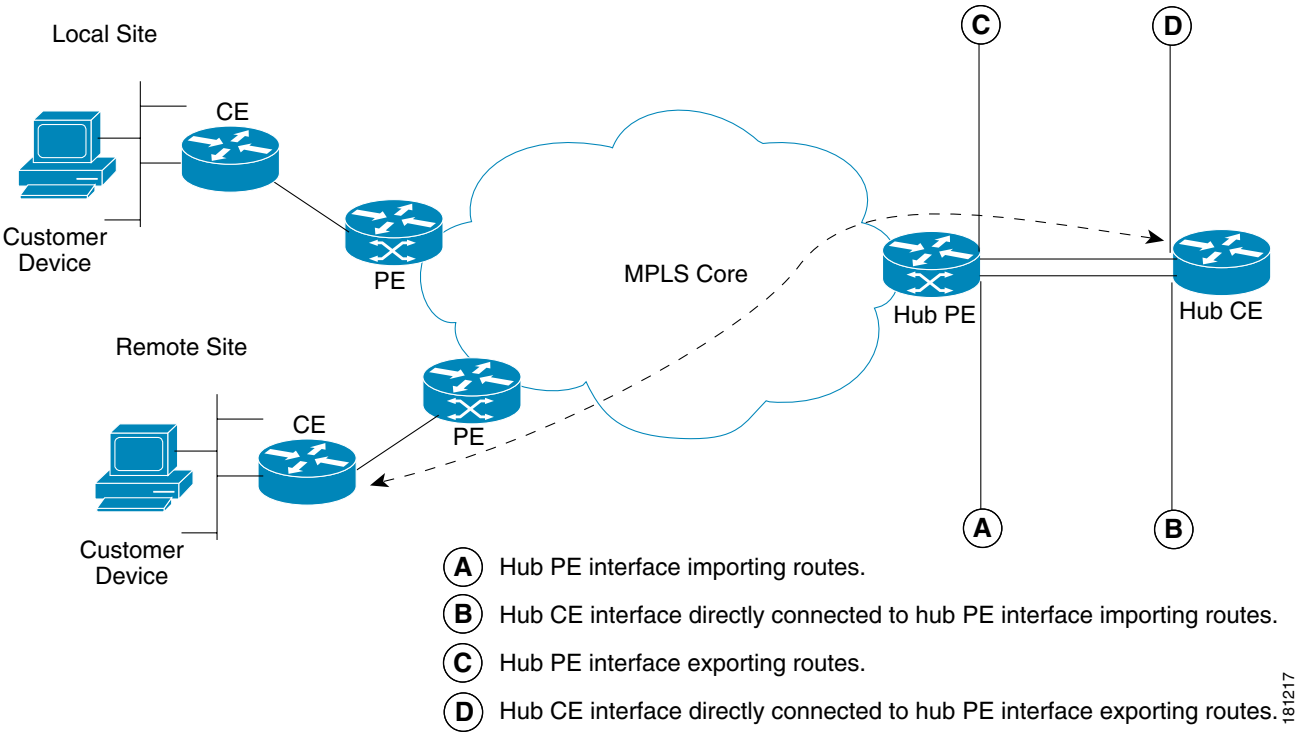
Field Name	Hub Detail
PE Device Name	Hub PE device name.
PE Access Circuit Interface	Hub PE interface which exports routes.
CE Access Circuit Interface IP Address	IP address of hub CE interface directly connected to PE interface which exports routes.
Customer Device IP Address	Leave blank.

Figure 62-5 Testing a Hub and Spoke VPN Topology—Step 4



5. You should perform an MPLS VPN Connectivity Verification test between the remote site (Spoke) and the hub CE interface that is attached to the hub PE interface which exports routes (shown in Figure 62-6 as *D*). When configuring the MPLS VPN Connectivity Verification test, the Local Site fields should be configured with details of the Hub PE/CE interfaces that export routes (shown in Figure 62-6 as *C* and *D*), as shown in Table 62-2. The Remote Site fields on the MPLS VPN Connectivity Verification Configuration window should be configured with details of the remote customer site.

Figure 62-6 Testing a Hub and Spoke VPN Topology—Step 5



Testing with Intranet/Extranet VPN Topology

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

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

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

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

Testing with Central Services VPN Topology

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

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