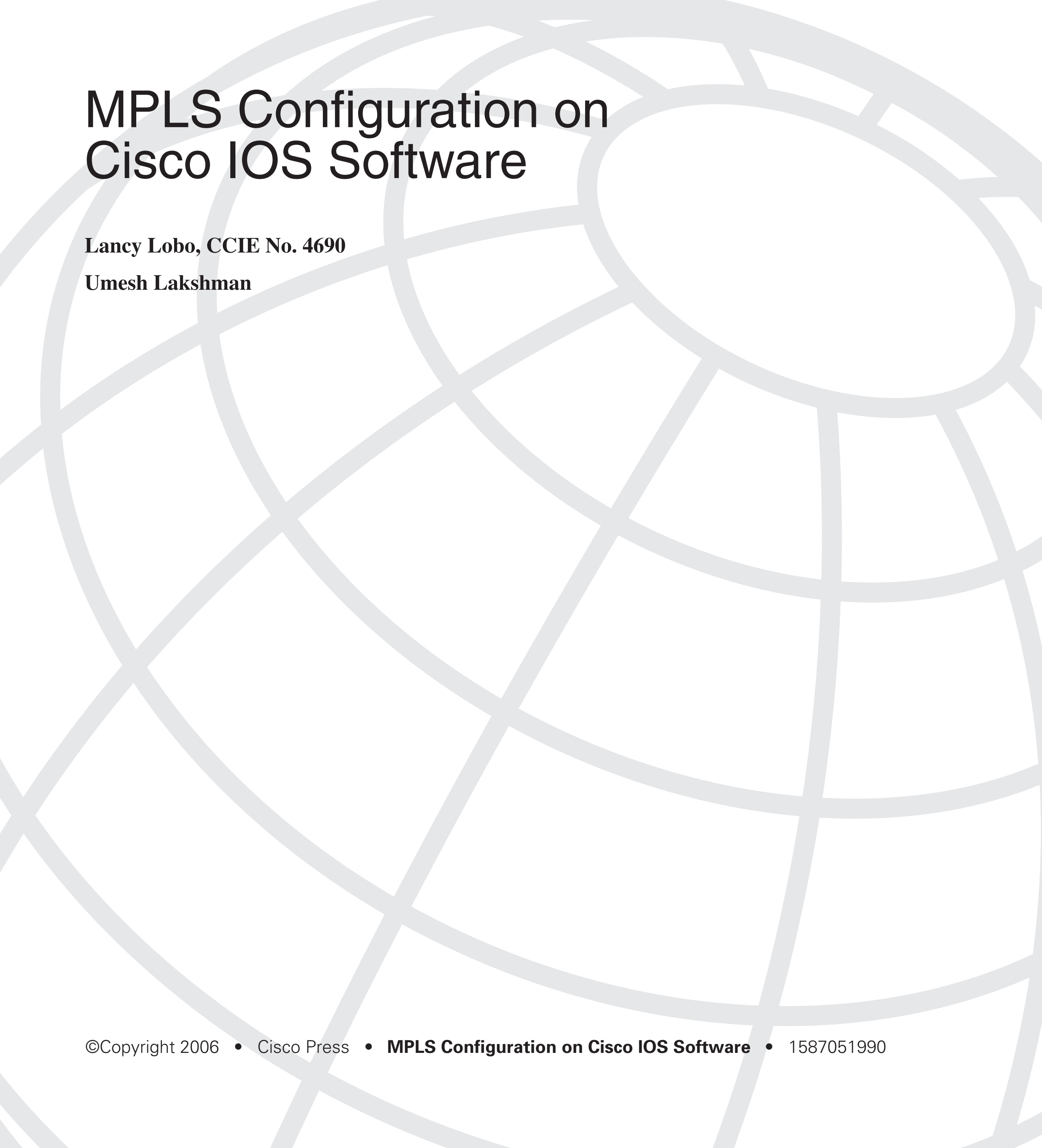


MPLS Configuration on Cisco IOS Software

Lancy Lobo, CCIE No. 4690

Umesh Lakshman

CHAPTER 15

Testing MPLS

This chapter addresses the procedures involved in testing a router for MPLS-related functionality using the three most popular testing tools or route/traffic generators available in the industry—Spirent Smartbits 6000, the IXIA 1600T, and the Agilent N2X.

First, an overview of the topology used to test MPLS functionality is provided, and then MPLS Layer 3 (L3) VPN, Layer 2 (L2) VPN, and VPLS are tested using the three traffic generators just mentioned. The tools are listed in alphabetical order.

Disclaimer

The intention of this chapter is to provide readers with procedures for testing L3 and L2 MPLS VPNs using the three most common test tools available in the market, namely, the Agilent N2X, the IXIA 1600T, and Spirent Smartbits 6000. This chapter provides a generic template for readers to use that can be scaled to meet different MPLS VPN scenarios in testing environments.

Testing L3 VPN with Agilent N2X

This section provides a step-by-step procedure to test L3 VPN functionality on a single device under test (DUT) using the Agilent N2X platform with the 6.4 software release.

The Agilent N2X system can be used for testing multilayer 10/100 Mbps Ethernet, Gigabit and 10 Gigabit Ethernet, ATM, and Packet over SONET switches, routers, and networks. The N2X product family includes the chassis, line cards, packets and protocols software program, and optional Tcl scripts and related software. The packets and protocols software provides complete configuration, control, and monitoring of all N2X resources in the test network, and the Tcl scripts allow the user to rapidly conduct the most popular industry benchmark tests.

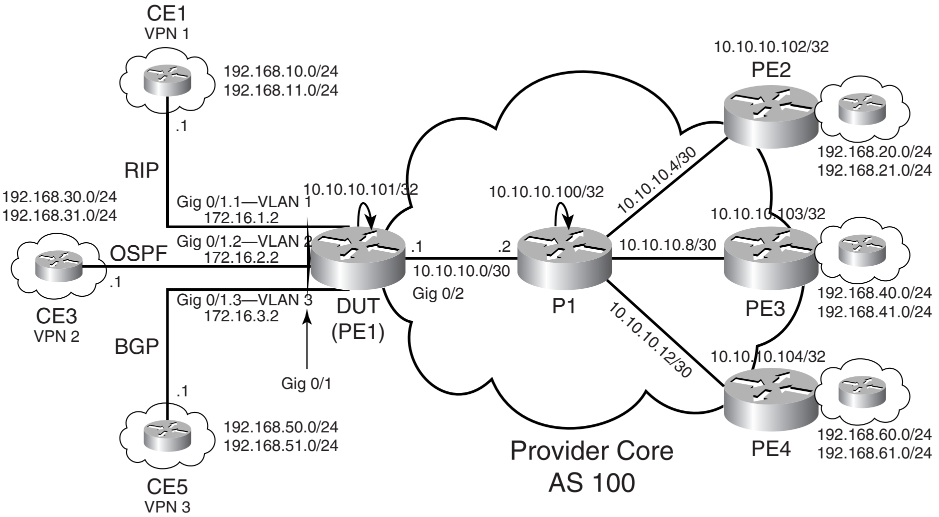
The user can configure and control the unit by the implementation of an external controller unit, which can be a PC with dual NIC cards where one Ethernet is connected to the back of the test set. The PC can then be connected to the management domain, and an administrator can remotely monitor and control it using the packets and protocols software program.

Multiple users can access the unit simultaneously, thereby splitting the ports within a chassis and controlling the activity and configuration of all ports and functions.

Topology for L3 VPN Testing

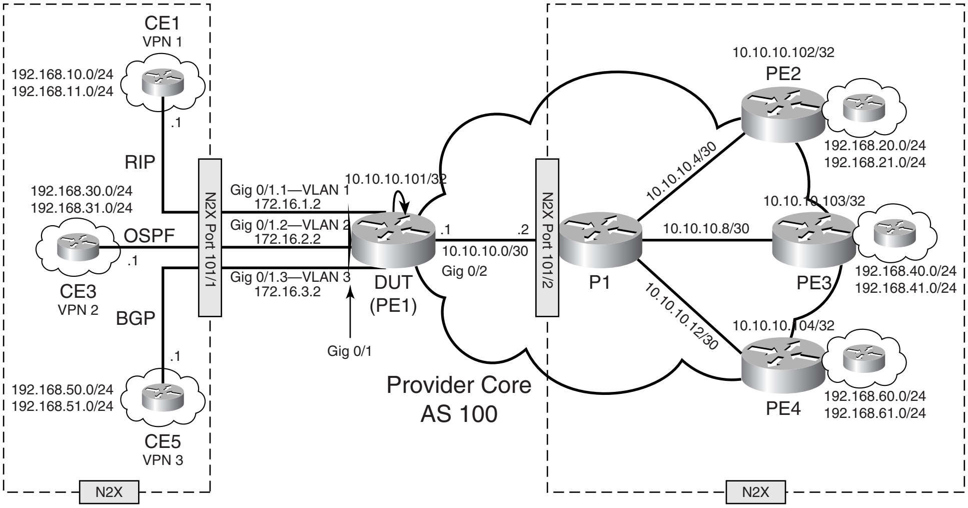
The topology used in the test setup attempts to emulate the network, as shown in Figure 15-1. A single Cisco router is configured to perform the functions of the Router PE1 in all test cases for L3 VPN. All other associated customer edge (CE) routers and core routers shown in Figure 15-1 are emulated using two test ports on each of the route/traffic generators.

Figure 15-1 *Topology*



All directly connected CE routers to PE1 in the topology shown in Figure 15-1 are emulated using logical links (sub-interfaces) with a single physical interface connecting to the route/traffic generator. A second link connecting to the PE from the route/traffic generators emulates the MPLS domain (consisting of Routers P1, PE2, PE3, and PE4) with the appropriate emulated PE routers advertising VPNv4 prefixes mapping to the networks to be advertised by Routers CE2, CE4, and CE6. In all route/traffic generators, no emulation of the remote PE-CE Routing protocol is performed. However, VPNv4 routes mapping to prefixes to be advertised by the remote CE routers are advertised by their directly connected emulated PE routers; for example, prefixes 192.168.20.0 and 21.0 to be advertised by CE Router CE2 will be emulated by advertising the same prefixes as part of VPN1 on PE2 as VPNv4 routes. The physical connectivity to emulate the network depicted in Figure 15-1 is illustrated in Figure 15-2.

Figure 15-2 *Physical Connectivity*



Testing L3 MPLS VPN Functionality

To test MPLS VPN PE functionality, a network is emulated, as shown in Figure 15-1, in which the DUT is PE1. The traffic generator and its ports are used to configure and emulate the rest of the network, as shown in Figure 15-2.

Conditions and Prerequisites

This test requires two ports on the route/traffic generator: one port to emulate CE connectivity to the DUT and the other port emulating the MPLS domain, which includes provider core routers and PE routers and remote CE routers belonging to multiple VPNs.

The test involves the emulation of three CE routers belonging to different VPNs, VPN1 to VPN3, connecting to the DUT using Gigabit Ethernet subinterfaces. Each VPN will generate prefixes, as shown in Figure 15-2.

RIP PE-CE will be implemented between PE1 and CE1 (VPN1), OSPF PE-CE will be implemented between PE1 and CE3 (VPN2), and BGP PE-CE will be implemented between PE1 and CE5 (VPN3).

Example 15-1 shows the configuration of the DUT used for testing MPLS VPN functionality.

Example 15-1 *DUT Configuration for L3 VPN Test*

```
hostname DUT
!
ip cef
!
ip vrf vpn1
rd 1:1
route-target export 1:1
route-target import 1:1
!
ip vrf vpn2
 rd 1:2
 route-target export 1:2
 route-target import 1:2
!
ip vrf vpn3
 rd 1:3
 route-target export 1:3
 route-target import 1:3
!
interface GigabitEthernet0/1
 description Connected to traffic generator port 1 (emulate local CE connections)
!
interface GigabitEthernet0/1.1
 encapsulation dot1Q 1
ip vrf forwarding vpn1
 ip address 172.16.1.2 255.255.255.0
!
interface GigabitEthernet0/1.2
 encapsulation dot1Q 2
 ip vrf forwarding vpn2
 ip address 172.16.2.2 255.255.255.0
!
interface GigabitEthernet0/1.3
 encapsulation dot1Q 3
 ip vrf forwarding vpn3
 ip address 172.16.3.2 255.255.255.0
!

interface GigabitEthernet0/2
 Description- Connection to Traffic Generator port 2 (emulate-MPLS domain)
 ip address 10.10.10.1 255.255.255.252
 mpls label protocol ldp
 mpls ip
!
router ospf 2 vrf vpn2
 log-adjacency-changes
 redistribute bgp 100 metric 10 subnets
 network 172.16.2.0 0.0.0.255 area 0
!
router ospf 100
 log-adjacency-changes
```

Example 15-1 *DUT Configuration for L3 VPN Test (Continued)*

```
 network 10.10.10.0 0.0.0.3 area 0
 network 10.10.10.101 0.0.0.0 area 0
!
router rip
 version 2
 !
 address-family ipv4 vrf vpn1
 network 172.16.0.0
 redistribute bgp 100
 no auto-summary
 version 2
 exit-address-family
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.10.10.102 remote-as 100
 neighbor 10.10.10.102 update-source loopback 0
 neighbor 10.10.10.103 remote-as 100
 neighbor 10.10.10.103 update-source loopback 0
 neighbor 10.10.10.104 remote-as 100
 neighbor 10.10.10.104 update-source loopback 0
no auto-summary
 !
 address-family vpnv4
 neighbor 10.10.10.102 activate
 neighbor 10.10.10.102 send-community extended
 neighbor 10.10.10.103 activate
 neighbor 10.10.10.103 send-community extended
 neighbor 10.10.10.104 activate
 neighbor 10.10.10.104 send-community extended
exit-address-family
 !
 address-family ipv4 vrf vpn3
 neighbor 172.16.3.1 remote-as 65001
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf vpn2
 redistribute ospf 2 vrf vpn2 metric 10
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf vpn1
 redistribute rip metric 3
 no auto-summary
 no synchronization
 exit-address-family
!
```

Testing L3 MPLS VPN Functionality with the N2X

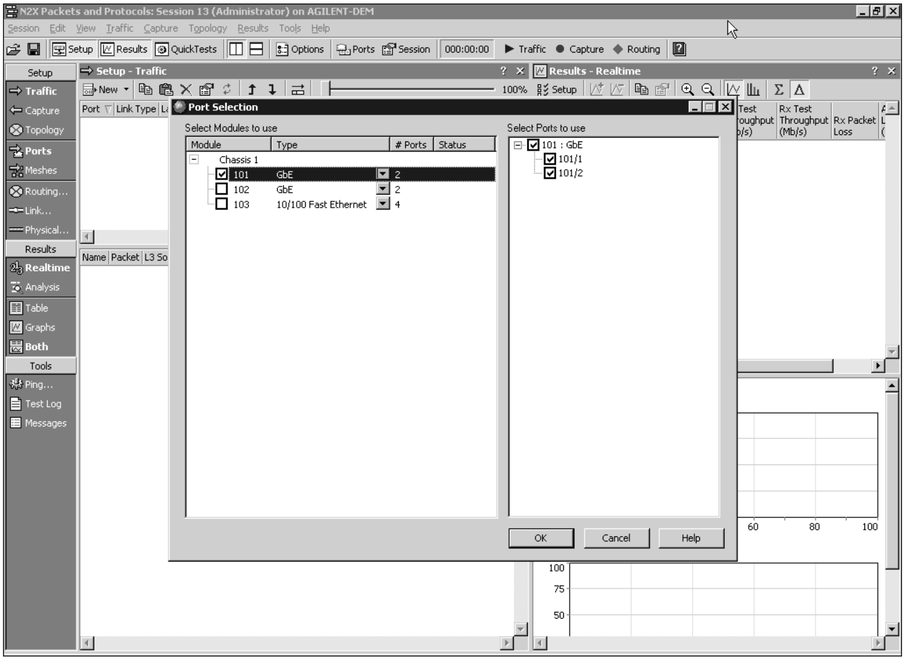
For the first test, use the N2X along with a two-port Gigabit Ethernet line card to test L3 VPN PE functionality of the DUT. For this test, all configurations for route as well as traffic generation are performed on the tool called the N2X Packets 6.4 System Release. The version used for all screenshots in this chapter is 6.4. Prior to all the configurations for this chapter, this software has to be installed on a client system that can then be used to remotely configure the N2X and cards. This will involve purchasing and installing the appropriate licenses and software, which can be procured by contacting your local sales representative. After installation, verify that the IP address assigned to the N2X chassis controller is reachable from the client system prior to configuration.

N2X Packets and Protocols Initial Configuration

After installation of the 6.4 release, the following steps are taken to test the DUT for L3 VPN functionality:

Step 1 Double-click the **N2X Packets 6.4 System Release** icon to start the program. This will open a window, as shown in Figure 15-3. Select the appropriate cards (in our case, 101) in the Port Selection window and click **OK**.

Figure 15-3 *Card Selection on Agilent*



Port Selection

Select Modules to use

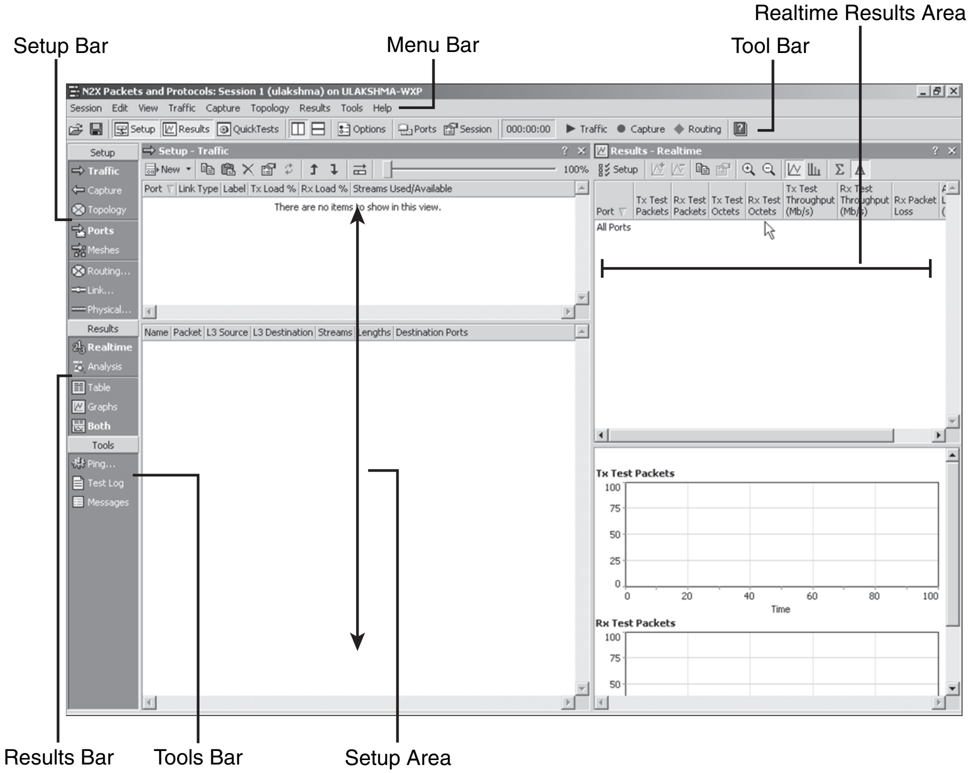
Module	Type	# Ports	Status
Chassis 1			
☑ 101	GbE	2	
☐ 102	GbE	2	
☐ 103	10/100 Fast Ethernet	4	

Select Ports to use

- ☑ 101 : GbE
  - ☑ 101/1
  - ☑ 101/2

Step 2 The main configuration window for the Agilent N2X chassis appears, as shown in Figure 15-4. The configuration panes for the N2X tool are also shown in Figure 15-4.

Figure 15-4 *N2X Packets and Protocols Configuration Panes*


Realtime Results Area
Setup Bar
Menu Bar
Tool Bar
N2X Packets and Protocols: Session 1 (ulakshma) on ULAKSHMA-WXP
Session Edit View Traffic Capture Topology Results Tools Help
Setup Results QuickTests Options Ports Session 000:00:00 Traffic Capture Routing
Setup
Traffic
Capture
Topology
Ports
Meshes
Routing...
Link...
Physical...
Results
Realtime
Analysis
Table
Graphs
Both
Tools
Ping...
Test Log
Messages
Setup - Traffic
New
100%
Port Link Type Label Tx Load % Rx Load % Streams Used/Available
There are no items to show in this view.
Name Packet L3 Source L3 Destination Streams Lengths Destination Ports
Results - Realtime
Setup
Port Tx Test Packets Rx Test Packets Tx Test Octets Rx Test Octets Tx Test Throughput (Mb/s) Rx Test Throughput (Mb/s) Rx Packet Loss
All Ports
Tx Test Packets
100
75
50
25
0
0
20
40
60
80
100
Time
Rx Test Packets
100
75
50
Results Bar
Tools Bar
Setup Area

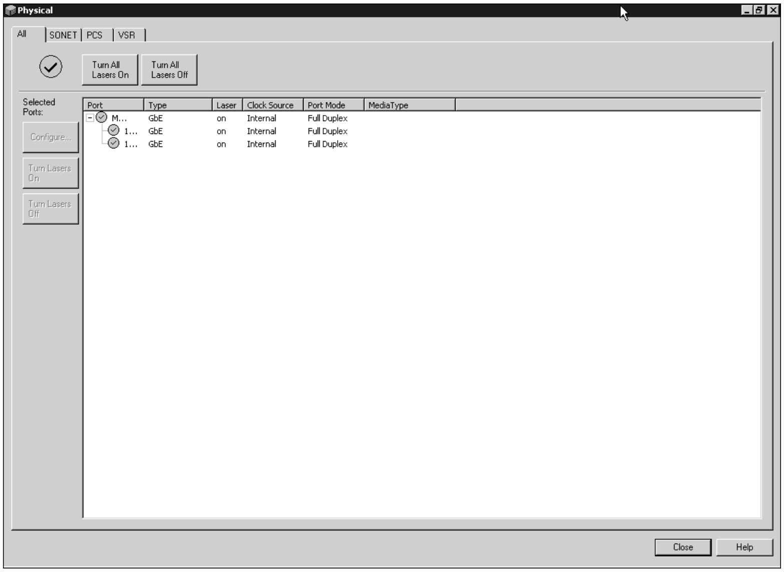
N2X Port Layer 1 (Physical) and Layer 2 (Link Layer) Configuration

This section outlines the steps to set up Layer 1 and Layer 2 connectivity between the DUT and the Agilent platform:

Step 1 To set up the Layer 1 connectivity on the Agilent N2X, click the **Physical** button in the Setup bar. This opens the Physical layer connection window, as shown in Figure 15-5. Check to see if all ports are denoted by a sign similar to the one depicted in Figure 15-5 (*black check mark in green circle*) that indicates the physical layer is connected.

Close the Physical layer window by clicking **Close** at the bottom of the window. If the *check mark in green circle* does not appear, you might have to click the **Turn Lasers On** button on the top of the Physical layer window to make the ports operational.

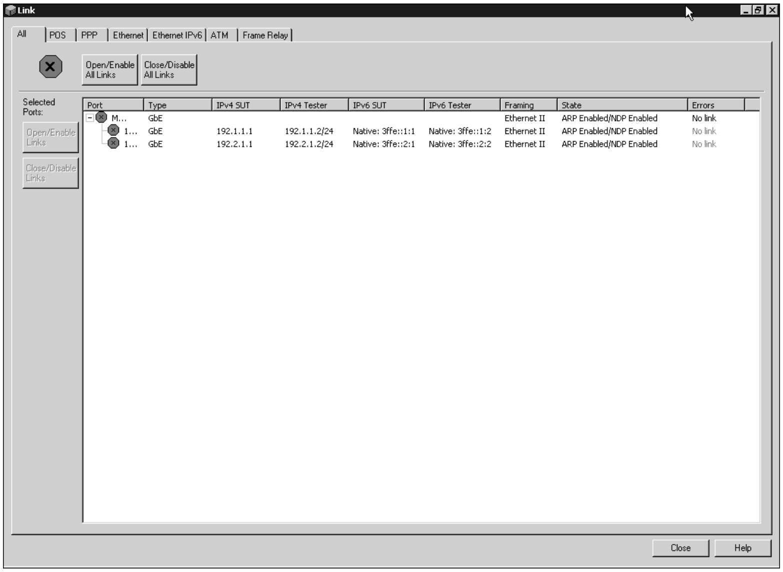
Figure 15-5 *Physical Layer*



Port	Type	Laser	Clock Source	Port Mode	MediaType
M…	GbE	on	Internal	Full Duplex	
1…	GbE	on	Internal	Full Duplex	
1…	GbE	on	Internal	Full Duplex	

Step 2 To set up Layer 2 connectivity on the Agilent N2X, click the **Link** button in the Setup bar. This opens the Link layer configuration window, as shown in Figure 15-6.

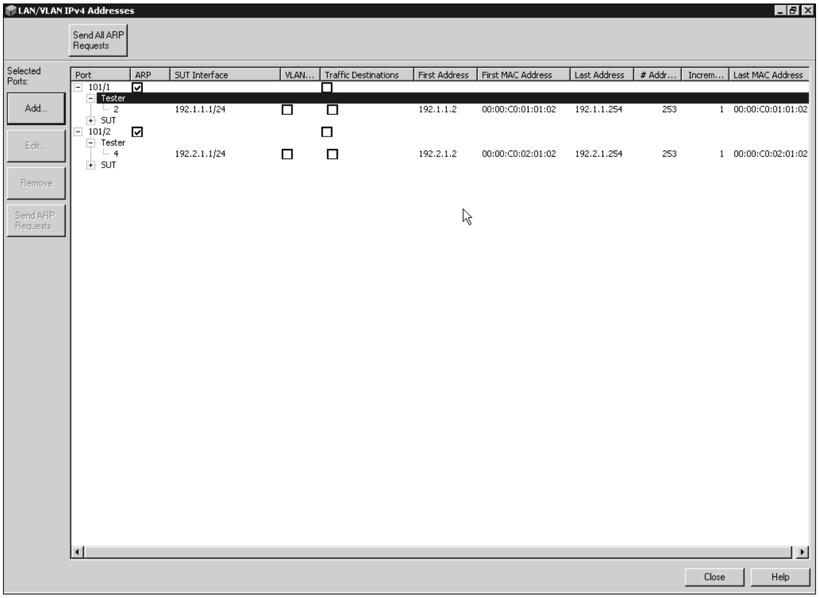
Figure 15-6 *Link Layer Configuration Window*



Port	Type	IPv4 SUT	IPv4 Tester	IPv6 SUT	IPv6 Tester	Framing	State	Errors
M…	GbE					Ethernet II	ARP Enabled/NDP Enabled	No link
1…	GbE	192.1.1.1	192.1.1.2/24	Native: 3ffe::1:1	Native: 3ffe::1:2	Ethernet II	ARP Enabled/NDP Enabled	No link
1…	GbE	192.2.1.1	192.2.1.2/24	Native: 3ffe::2:1	Native: 3ffe::2:2	Ethernet II	ARP Enabled/NDP Enabled	No link

Click the **Ethernet** tab in the Link layer window. Under the Ethernet tab, click the **LAN/VLAN Addresses** button. This opens a new LAN/VLAN IPv4 Addresses window that enables you to configure the VLAN IP addresses for the CE connections as well as the DUT to Tester connections for the core emulation port. The LAN/VLAN IPv4 Addresses window is shown in Figure 15-7.

Figure 15-7 *LAN/VLAN IP Configuration Window*

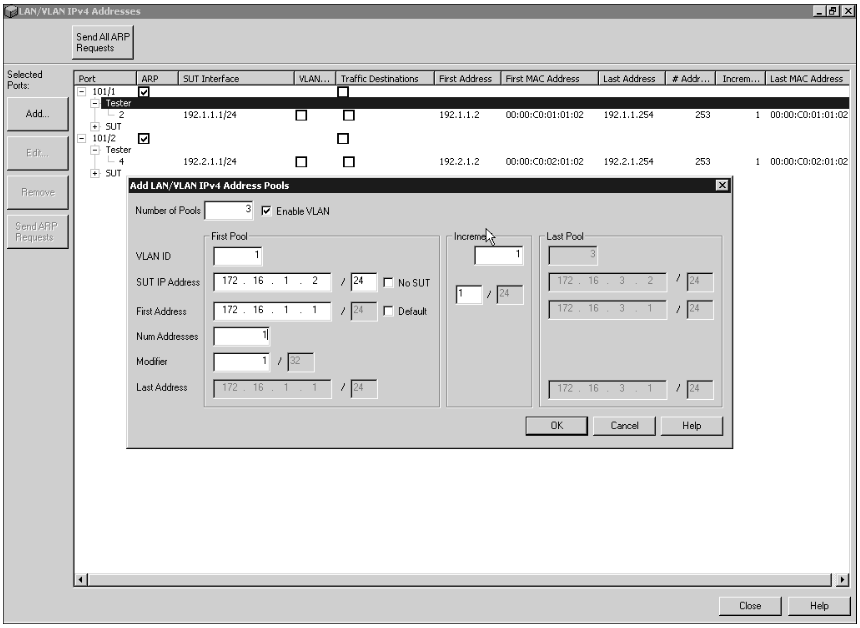


Port	ARP	SUT Interface	VLAN...	Traffic Destinations	First Address	First MAC Address	Last Address	# Addr...	Increm...	Last MAC Address
101/1	☑			☐						
Tester										
2		192.1.1.1/24	☐	☐	192.1.1.2	00:00:C0:01:01:02	192.1.1.254	253	1	00:00:C0:01:01:02
SUT										
101/2	☑			☐						
Tester										
4		192.2.1.1/24	☐	☐	192.2.1.2	00:00:C0:02:01:02	192.2.1.254	253	1	00:00:C0:02:01:02
SUT										

Port 101/1 will be used to emulate CE Routers CE1, CE3 and CE5. Under Port 101/1, click the **Tester** row and click **Add** in the main LAN/VLAN IPv4 Addresses window. This will open the Add LAN/VLAN IP Address Pools window. In the window, perform the configuration as shown in Figure 15-8 by setting the number of pools to 3 and enabling VLANs where the first SUT IP address is 172.16.1.2 and the first address of tester (not Default) is configured to be 172.16.1.1 with a total of one address per pool. After entering these values, the last pool (for CE3) is depicted in the other half of the IP address pool configuration window, as indicated in Figure 15-8. Click **OK**.

This process adds three interfaces for the CE-PE (DUT) connections as required by the setups illustrated in Figure 15-9 in the LAN/VLAN IP configuration window under Tester for Port 101/1. Remove the default interface created on Port 101/1 by highlighting the same in the window and clicking **Remove** (not shown).

Figure 15-8 *LAN/VLAN IP Configuration: CE Emulation on 101/1*



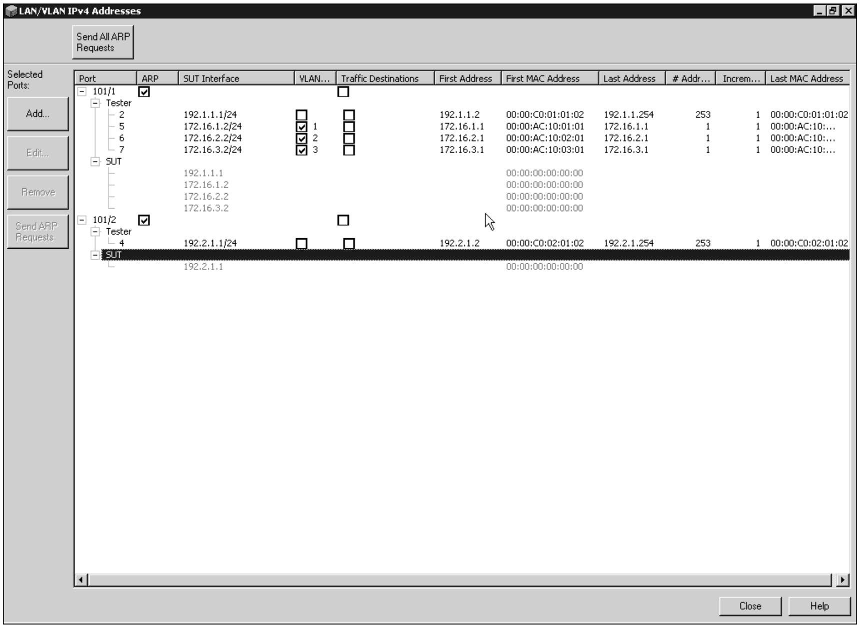
Port	ARP	SUT Interface	VLAN...	Traffic Destinations	First Address	First MAC Address	Last Address	# Addr...	Increm...	Last MAC Address
101/1	☑			☐						
Tester										
2		192.1.1.1/24	☐	☐	192.1.1.2	00:00:C0:01:01:02	192.1.1.254	253	1	00:00:C0:01:01:02
SUT										
101/2	☑			☐						
Tester										
4		192.2.1.1/24	☐	☐	192.2.1.2	00:00:C0:02:01:02	192.2.1.254	253	1	00:00:C0:02:01:02
SUT										

Add LAN/VLAN IPv4 Address Pools

Number of Pools 3 ☑ Enable VLAN

	First Pool	Increme	Last Pool
VLAN ID	1	1	3
SUT IP Address	172 . 16 . 1 . 2 / 24 ☐ No SUT	1 / 24	172 . 16 . 3 . 2 / 24
First Address	172 . 16 . 1 . 1 / 24 ☐ Default		172 . 16 . 3 . 1 / 24
Num Addresses	1		
Modifier	1 / 32		
Last Address	172 . 16 . 1 . 1 / 24		172 . 16 . 3 . 1 / 24

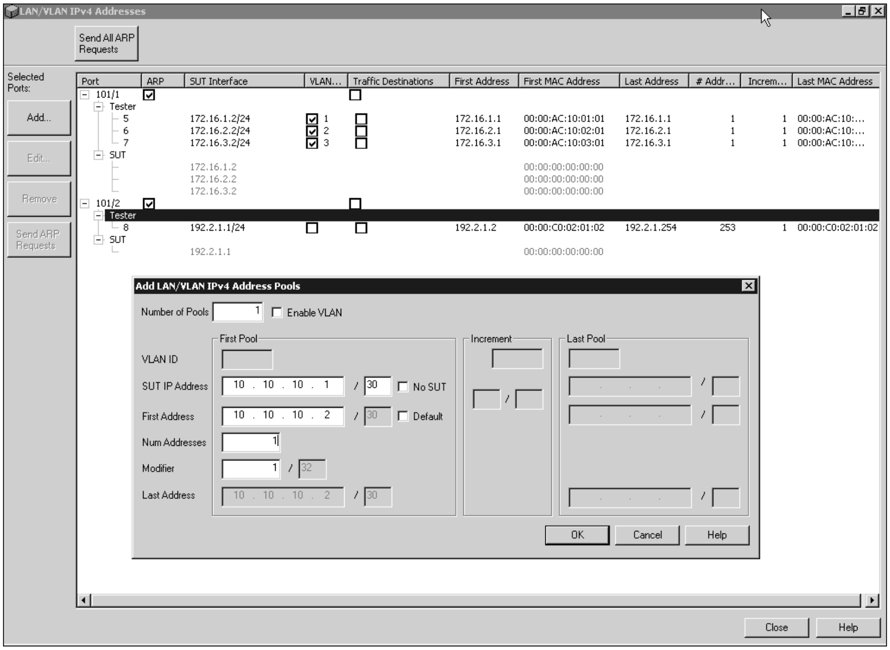
Figure 15-9 *LAN/VLAN IP Configuration: CE Configuration*



Port	ARP	SUT Interface	VLAN...	Traffic Destinations	First Address	First MAC Address	Last Address	# Addr...	Increm...	Last MAC Address
101/1	☑			☐						
Tester										
2		192.1.1.1/24	☐	☐	192.1.1.2	00:00:C0:01:01:02	192.1.1.254	253	1	00:00:C0:01:01:02
5		172.16.1.2/24	☑ 1	☐	172.16.1.1	00:00:AC:10:01:01	172.16.1.1	1	1	00:00:AC:10:...
6		172.16.2.2/24	☑ 2	☐	172.16.2.1	00:00:AC:10:02:01	172.16.2.1	1	1	00:00:AC:10:...
7		172.16.3.2/24	☑ 3	☐	172.16.3.1	00:00:AC:10:03:01	172.16.3.1	1	1	00:00:AC:10:...
SUT										
		192.1.1.1				00:00:00:00:00:00				
		172.16.1.2				00:00:00:00:00:00				
		172.16.2.2				00:00:00:00:00:00				
		172.16.3.2				00:00:00:00:00:00				
101/2	☑			☐						
Tester										
4		192.2.1.1/24	☐	☐	192.2.1.2	00:00:C0:02:01:02	192.2.1.254	253	1	00:00:C0:02:01:02
SUT										
		192.2.1.1				00:00:00:00:00:00				

Step 3 Repeat the procedure in Step 2 to configure Port 101/2. This port is used to emulate the connection from the DUT/SUT to the emulated core and PE routers. Figure 15-10 depicts the configuration process.

Figure 15-10 *LAN/VLAN IP Configuration: Core Emulation on 101/2*



Port	ARP	SUT Interface	VLAN...	Traffic Destinations	First Address	First MAC Address	Last Address	# Addr...	Increm...	Last MAC Address
101/1	☑			☐						
Tester										
5		172.16.1.2/24	☑ 1	☐	172.16.1.1	00:00:AC:10:01:01	172.16.1.1	1	1	00:00:AC:10:...
6		172.16.2.2/24	☑ 2	☐	172.16.2.1	00:00:AC:10:02:01	172.16.2.1	1	1	00:00:AC:10:...
7		172.16.3.2/24	☑ 3	☐	172.16.3.1	00:00:AC:10:03:01	172.16.3.1	1	1	00:00:AC:10:...
SUT										
		172.16.1.2				00:00:00:00:00:00				
		172.16.2.2				00:00:00:00:00:00				
		172.16.3.2				00:00:00:00:00:00				
101/2	☑			☐						
Tester										
8		192.2.1.1/24	☐	☐	192.2.1.2	00:00:C0:02:01:02	192.2.1.254	253	1	00:00:C0:02:01:02
SUT										
		192.2.1.1				00:00:00:00:00:00				

Number of Pools 1 ☐ Enable VLAN

First Pool
VLAN ID
SUT IP Address 10 . 10 . 10 . 1 / 30 ☐ No SUT
First Address 10 . 10 . 10 . 2 / 30 ☐ Default
Num Addresses 1
Modifier 1 / 32
Last Address 10 . 10 . 10 . 2 / 30

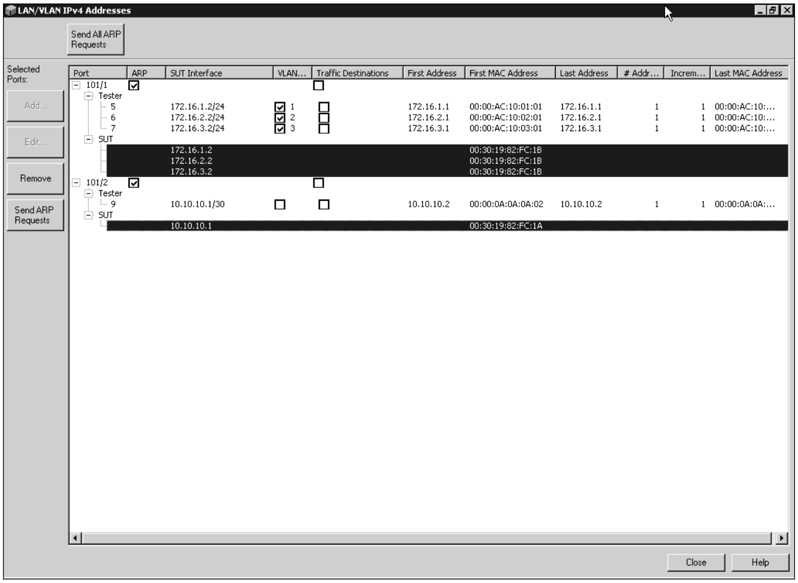
Increment

Last Pool

Step 4 Once the configuration for both ports is complete, click the **Send ARP Requests** button in the LAN/VLAN IPv4 Addresses window. If all other port configurations are performed correctly on the DUT/SUT, the ARP entries for the ports on the SUT side populate, as shown by the highlighted entries in Figure 15-11.

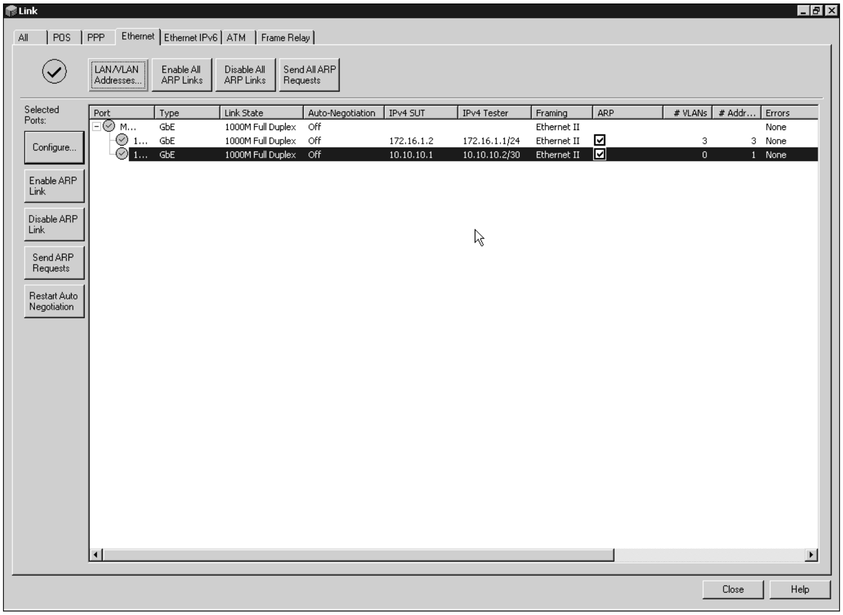
Step 5 Close the LAN/VLAN IPv4 Addresses window by clicking **Close**. The screen will now show the Link layer window with both ports up, illustrated by the check mark in green circle next to each port, as shown in Figure 15-12. Close the Link layer window by clicking **Close**.

Figure 15-11 *LAN IP Configuration: ARP*



Port	ARP	SUT Interface	VLAN...	Traffic Destinations	First Address	First MAC Address	Last Address	# Addr...	Increm...	Last MAC Address
101/1	☑			☐						
Tester										
5		172.16.1.2/24	☑ 1	☐	172.16.1.1	00:00:AC:10:01:01	172.16.1.1	1	1	00:00:AC:10:...
6		172.16.2.2/24	☑ 2	☐	172.16.2.1	00:00:AC:10:02:01	172.16.2.1	1	1	00:00:AC:10:...
7		172.16.3.2/24	☑ 3	☐	172.16.3.1	00:00:AC:10:03:01	172.16.3.1	1	1	00:00:AC:10:...
SUT										
		172.16.1.2				00:30:19:82:FC:1B				
		172.16.2.2				00:30:19:82:FC:1B				
		172.16.3.2				00:30:19:82:FC:1B				
101/2	☑			☐						
Tester										
9		10.10.10.1/30	☐	☐	10.10.10.2	00:00:0A:0A:0A:02	10.10.10.2	1	1	00:00:0A:0A:...
SUT										
		10.10.10.1				00:30:19:82:FC:1A				

Figure 15-12 *Layer 2 Configuration Complete*



Port	Type	Link State	Auto-Negotiation	IPv4 SUT	IPv4 Tester	Framing	ARP	# VLANs	# Addr...	Errors
M...	GbE	1000M Full Duplex	Off			Ethernet II				None
1...	GbE	1000M Full Duplex	Off	172.16.1.2	172.16.1.1/24	Ethernet II	☑	3	3	None
1...	GbE	1000M Full Duplex	Off	10.10.10.1	10.10.10.2/30	Ethernet II	☑	0	1	None

N2X RIP PE-CE Configuration

The following steps outline the implementation of RIP PE-CE between the DUT and the emulated CE1 router:

Step 1 In the following three steps, you will configure the CE interfaces for RIP PE-CE routing for VPN1.

(a) Click the **Routing** button in the Setup pane. This will open the Routing window shown in Figure 15-13.

(b) Select the **RIP** tab.

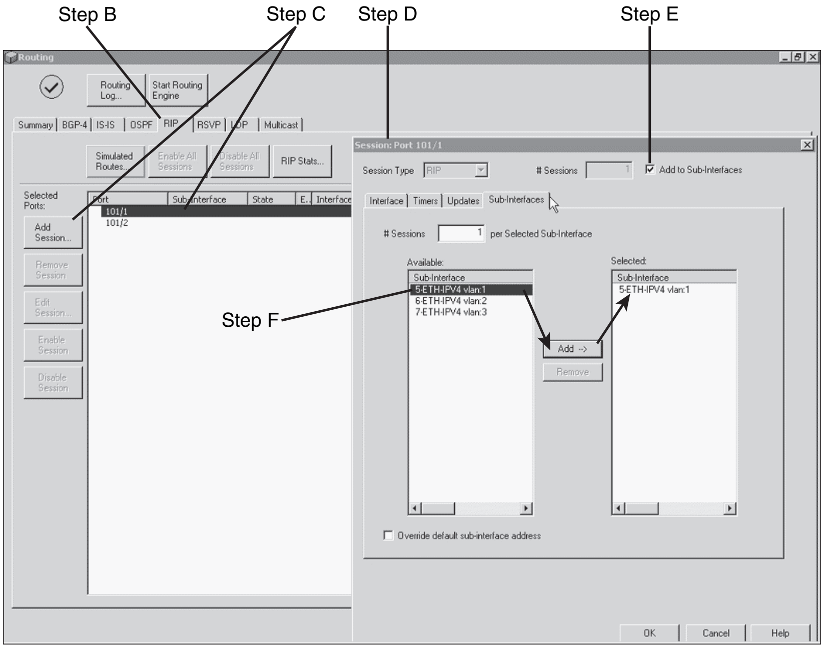
(c) Highlight Port **101/1** in the window and click **Add Session**.

(d) This will open the Session window for Port 101/1.

(e) In the Session window, put a check mark in the **Add to Sub-Interfaces**, which will automatically take you to the Sub-Interfaces tab.

(f) Select **5-ETH-IPV4 vlan:1**, which is the sub-interface mapping to the CE1 connection in the Available Sub-Interfaces window, and click **Add** to add the same to the selected sub-interfaces.

Figure 15-13 *RIP PE-CE Configuration*



Port: 101/1, 101/2

Session Type: RIP

# Sessions: 1

☑ Add to Sub-Interfaces

# Sessions 1 per Selected Sub-Interface

Available: 5-ETH-IPV4 vlan:1, 6-ETH-IPV4 vlan:2, 7-ETH-IPV4 vlan:3

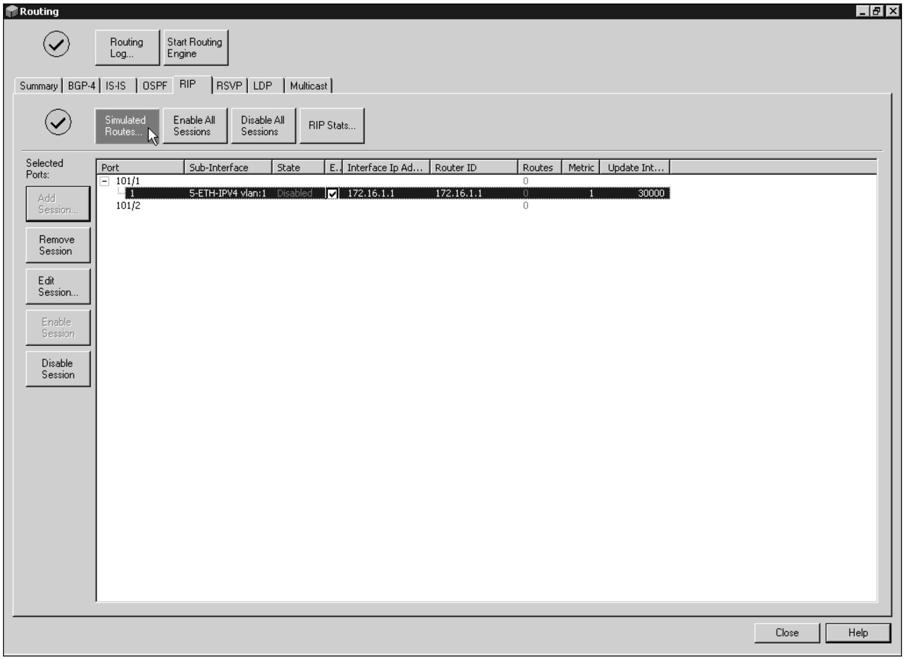
Selected: 5-ETH-IPV4 vlan:1

☐ Override default sub-interface address

(g) Click **OK** in the Session window.

(h) Highlight the newly added session in the Routing window and click the **Simulated Routes** button, as shown in Figure 15-14.

Figure 15-14 *RIP PE-CE Configuration—Simulating CE Routes*



Port	Sub-Interface	State	E..	Interface Ip Ad...	Router ID	Routes	Metric	Update Int...
101/1						0		
1	5-ETH-IPV4 vlan:1	Disabled	☑	172.16.1.1	172.16.1.1	0	1	30000
101/2						0		

Step 2 The RIP Simulated Routes window opens.

(a) Highlight the session under Port 101/1.

(b) Click **Add Route Pools**. This opens the Route Pools configuration window.

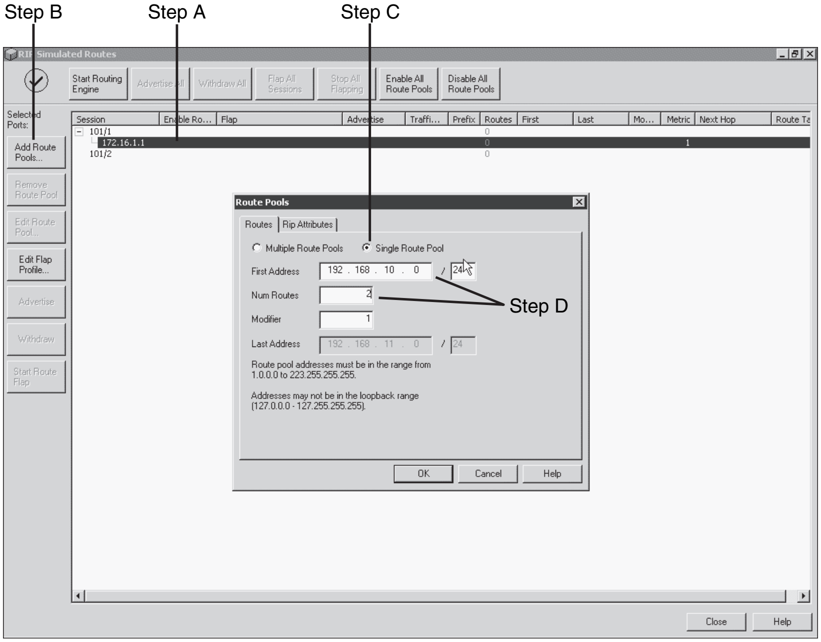
(c) Select **Single Route Pool**.

(d) Enter appropriate values into the Route Pools configuration window to generate prefixes 192.168.10.0 and 192.168.11.0, as shown in Figure 15-15.

(e) Click **OK**.

Step 3 This configuration will create a route pool as required by the setup illustrated in Figure 15-16.

Figure 15-15 *RIP PE-CE: Route Pool Configuration*



Session	Enable Ro...	Flap	Advertise	Traffi...	Prefix	Routes	First	Last	Mo...	Metric	Next Hop	Route Ta
101/1						0						
172.16.1.1						0				1		
101/2						0						

○ Multiple Route Pools ● Single Route Pool

First Address 192 . 168 . 10 . 0 / 24

Num Routes 2

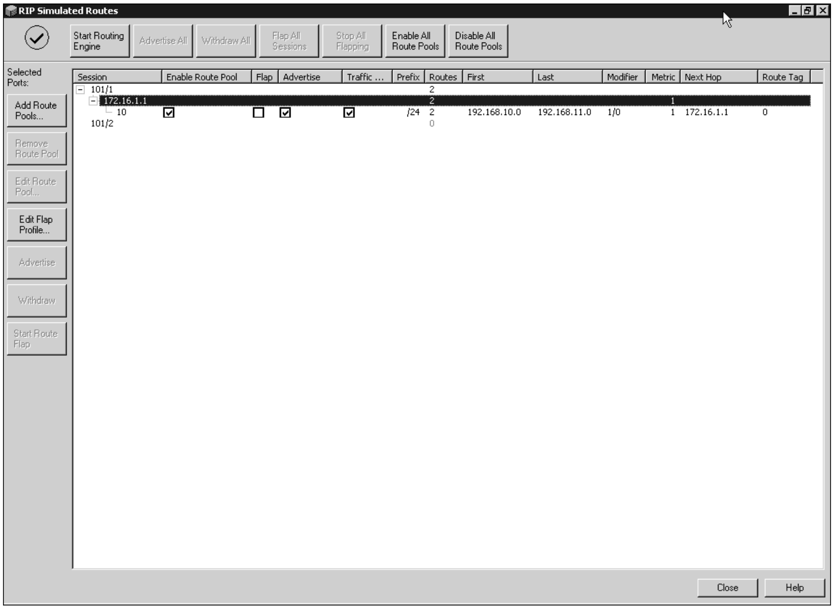
Modifier 1

Last Address 192 . 168 . 11 . 0 / 24

Route pool addresses must be in the range from 1.0.0.0 to 223.255.255.255.

Addresses may not be in the loopback range (127.0.0.0 - 127.255.255.255).

Figure 15-16 *RIP PE-CE Complete Route Configuration*

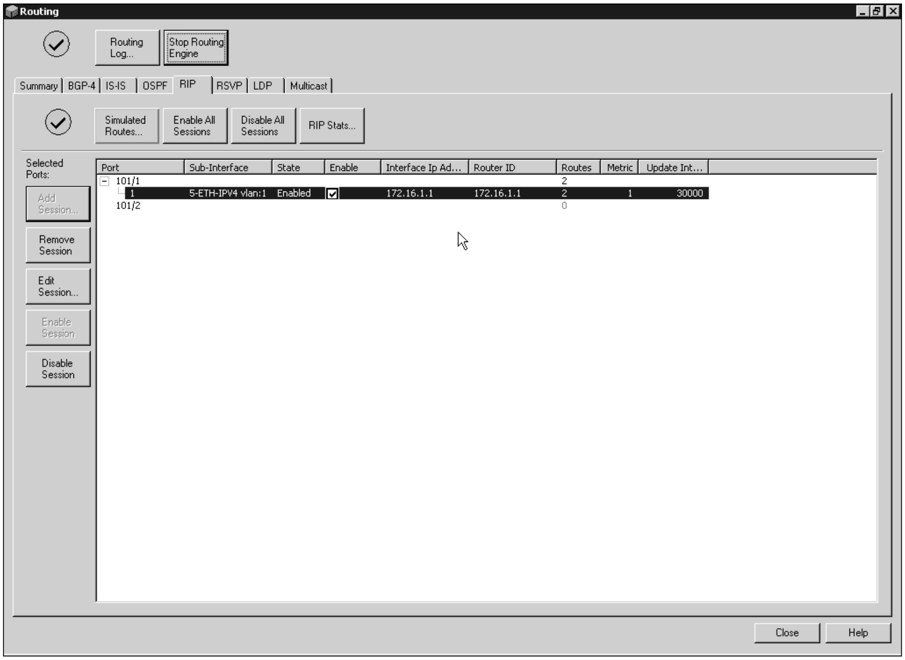


Session	Enable Route Pool	Flap	Advertise	Traffic ...	Prefix	Routes	First	Last	Modifier	Metric	Next Hop	Route Tag
101/1						2						
172.16.1.1						2				1		
10	☑	☐	☑	☑	/24	2	192.168.10.0	192.168.11.0	1/0	1	172.16.1.1	0
101/2						0						

Step 4 Click **Close** to close the RIP Simulated Routes configuration window.

Step 5 In the Routing window, click **Enable All Sessions** and then click **Start Routing Engine**. The state of the session must change from Disabled to Enabled, as shown in Figure 15-17. The verification of RIP PE-CE operation is shown in Example 15-2.

Figure 15-17 *RIP PE-CE States*



Port	Sub-Interface	State	Enable	Interface Ip Ad...	Router ID	Routes	Metric	Update Int...
101/1						2		
1	5-ETH-IPV4 vlan:1	Enabled	☑	172.16.1.1	172.16.1.1	2	1	30000
101/2						0		

Example 15-2 *DUT Verification of RIP PE-CE*

```
DUT#show ip route vrf vpn1 rip
R    192.168.10.0/24 [120/1] via 172.16.1.1, 00:00:28, GigabitEthernet0/1.1
R    192.168.11.0/24 [120/1] via 172.16.1.1, 00:00:28, GigabitEthernet0/1.1
```

N2X OSPF PE-CE and OSPF IGP Configuration

The following steps illustrate implementation of OSPF PE-CE between the DUT and the emulated CE2 router:

Step 1 To configure OSPF, select the **OSPF** tab under the Routing window, as shown in Figure 15-18.

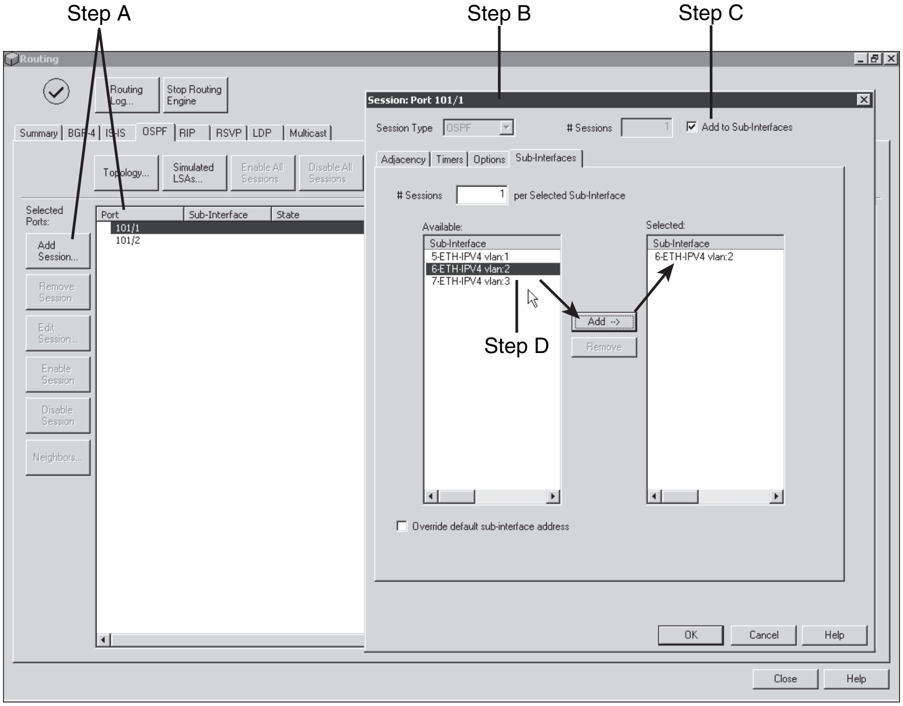
(a) Highlight Port 101/1 in the window and click **Add Session**.

(b) This will open the Session window for Port 101/1.

(c) In the Session window, check mark **Add to Sub-Interfaces**, which will automatically take you to the Sub-Interfaces tab.

(d) Select **5-ETH-IPV4 vlan:2**, which is the sub-interface mapping to the CE2 connection in the Available Sub-Interfaces window, and click **Add** to add the same to the selected sub-interfaces.

Figure 15-18 *OSPF PE-CE Configuration*



Session Type: OSPF

Sessions: 1

☑ Add to Sub-Interfaces

Sessions: 1 per Selected Sub-Interface

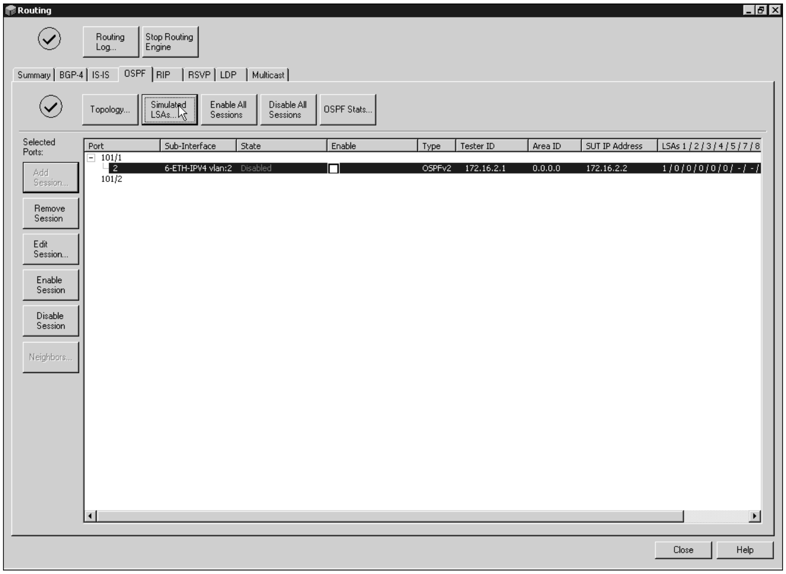
Selected: 6-ETH-IPV4 vlan:2

☐ Override default sub-interface address

(e) Click **OK** in the Session window.

(f) Highlight the newly added session in the Routing window and click the **Simulated LSAs** button, as shown in Figure 15-19.

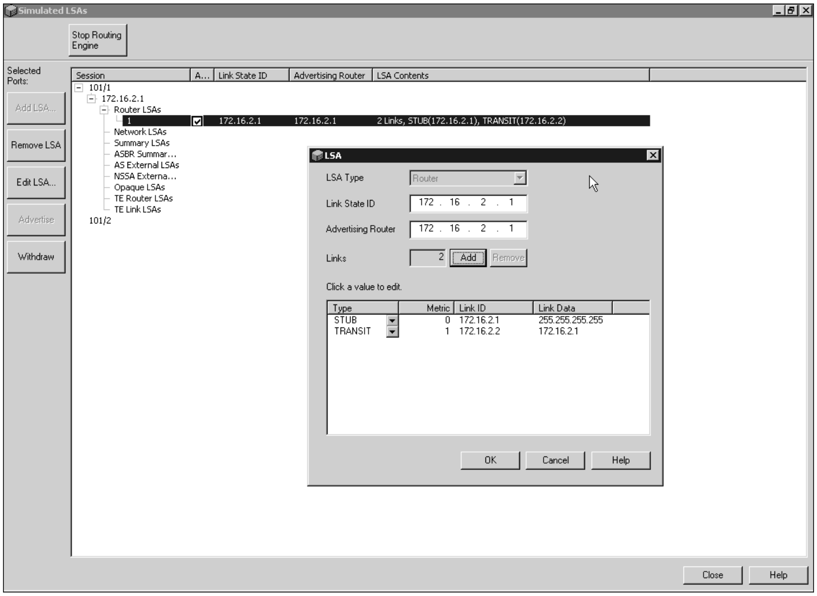
Figure 15-19 *OSPF PE-CE-LSAs*



Port	Sub-Interface	State	Enable	Type	Tester ID	Area ID	SUT IP Address	LSAs 1 / 2 / 3 / 4 / 5 / 7 / 8
101/1								
2	6-ETH-IPV4 vlan:2	Disabled	☐	OSPFv2	172.16.2.1	0.0.0.0	172.16.2.2	1 / 0 / 0 / 0 / 0 / 0 / - / - /
101/2								

Step 2 In the Simulated LSAs window, highlight the Router LSA under the session on Port 101/1 and click **Edit LSA** to open the LSA window, as shown in Figure 15-20.

Figure 15-20 *Edit Router LSAs*



Session	A...	Link State ID	Advertising Router	LSA Contents
101/1				
172.16.2.1				
Router LSAs				
1	☑	172.16.2.1	172.16.2.1	2 Links, STUB(172.16.2.1), TRANSIT(172.16.2.2)
Network LSAs				
Summary LSAs				
ASBR Summar...				
AS External LSAs				
NSSA Externa...				
Opaque LSAs				
TE Router LSAs				
TE Link LSAs				
101/2				

LSA Type: Router

Link State ID: 172 . 16 . 2 . 1

Advertising Router: 172 . 16 . 2 . 1

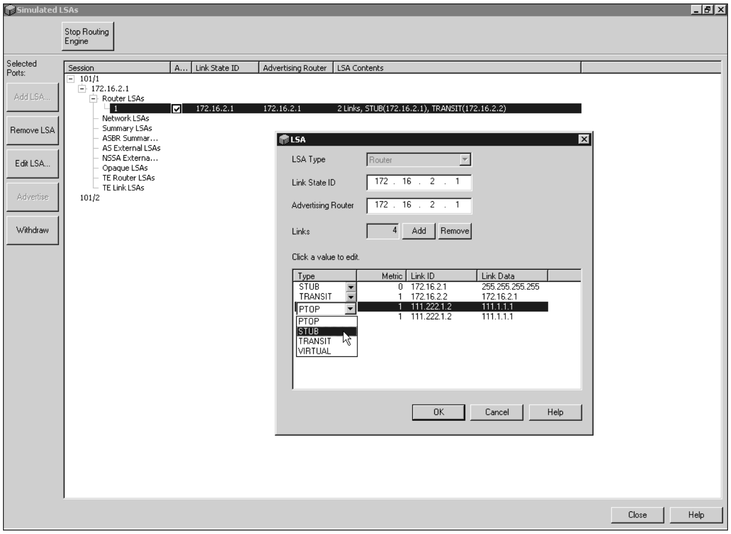
Links: 2 Add Remove

Click a value to edit.

Type	Metric	Link ID	Link Data
STUB	0	172.16.2.1	255.255.255.255
TRANSIT	1	172.16.2.2	172.16.2.1

Step 3 In the LSA window, click **Add** two times to add the two networks to be advertised by OSPF (192.168.30.0 and 31.0/24). Select **STUB** from the drop-down menu under Type in the LSA window, as shown in Figure 15-21.

Figure 15-21 *OSPF PE-CE: Adding Networks*



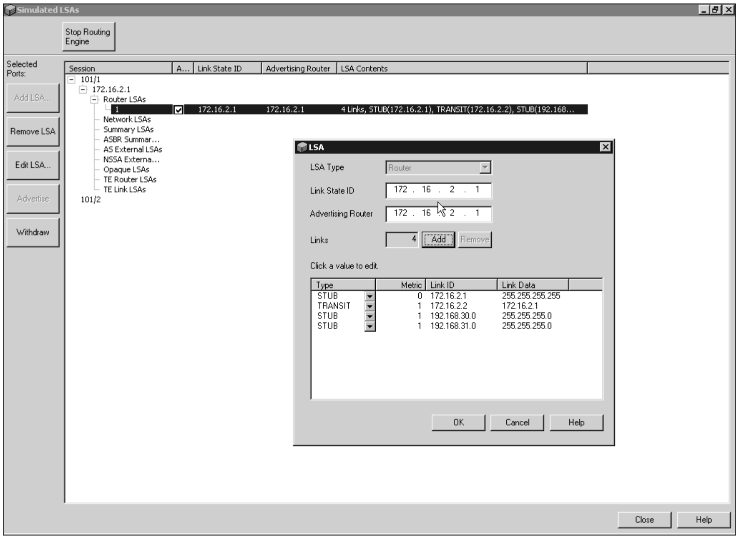
Session	A...	Link State ID	Advertising Router	LSA Contents
101/1				
172.16.2.1				
Router LSAs				
1	☑	172.16.2.1	172.16.2.1	2 Links, STUB(172.16.2.1), TRANSIT(172.16.2.2)

LSA Type: Router
Link State ID: 172 . 16 . 2 . 1
Advertising Router: 172 . 16 . 2 . 1
Links: 4

Type	Metric	Link ID	Link Data
STUB	0	172.16.2.1	255.255.255.255
TRANSIT	1	172.16.2.2	172.16.2.1
PTOP	1	111.222.1.2	111.1.1.1
	1	111.222.1.2	111.1.1.1

Step 4 Configure the appropriate values for the Link State ID and Advertising Router for the two networks, as shown in Figure 15-22.

Figure 15-22 *OSPF PE-CE: Configuring CE Networks*



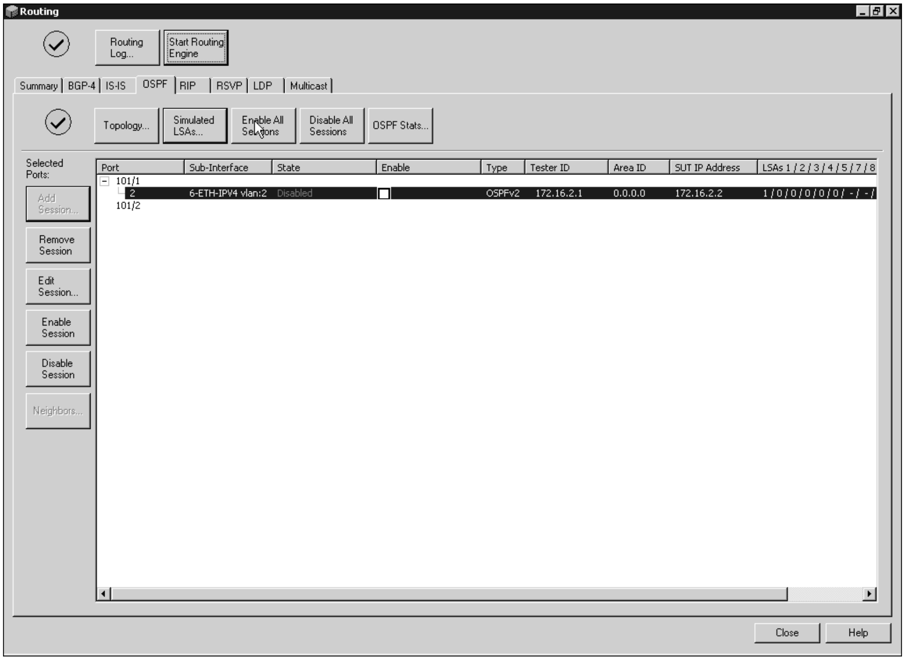
Session	A...	Link State ID	Advertising Router	LSA Contents
101/1				
172.16.2.1				
Router LSAs				
1	☑	172.16.2.1	172.16.2.1	4 Links, STUB(172.16.2.1), TRANSIT(172.16.2.2), STUB(192.168...

LSA Type: Router
Link State ID: 172 . 16 . 2 . 1
Advertising Router: 172 . 16 . 2 . 1
Links: 4

Type	Metric	Link ID	Link Data
STUB	0	172.16.2.1	255.255.255.255
TRANSIT	1	172.16.2.2	172.16.2.1
STUB	1	192.168.30.0	255.255.255.0
STUB	1	192.168.31.0	255.255.255.0

Step 5 Click **OK** to close the LSA window and **Close** to close the Simulated LSA window. To enable this session, stop the routing engine by clicking on the **Stop Routing Engine** button in the Routing window and then clicking on **Enable All Sessions**, as shown in Figure 15-23.

Figure 15-23 *OSPF PE-CE: Enabling CE Sessions*



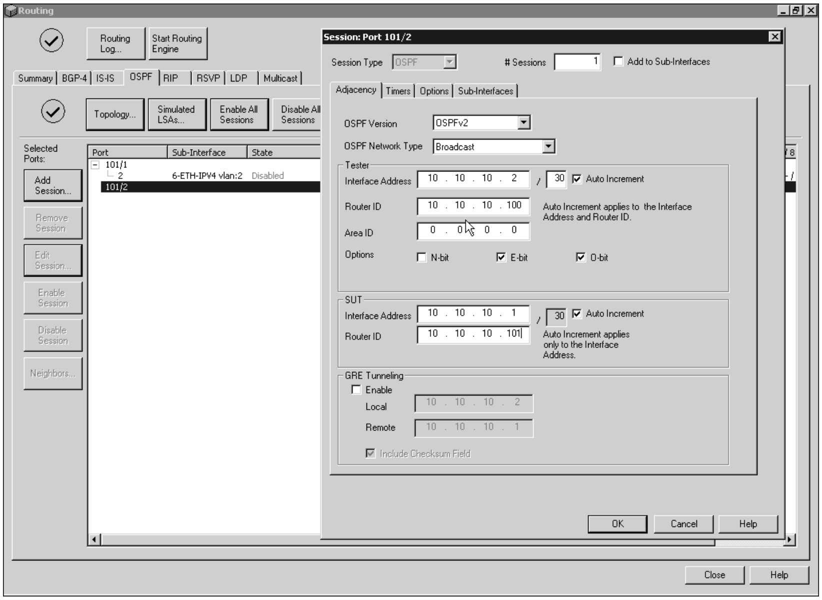
Port	Sub-Interface	State	Enable	Type	Tester ID	Area ID	SUT IP Address	LSAs 1 / 2 / 3 / 4 / 5 / 7 / 8
101/1								
2	6-ETH-IPV4 vlan:2	Disabled	☐	OSPFv2	172.16.2.1	0.0.0.0	172.16.2.2	1 / 0 / 0 / 0 / 0 / 0 / - / - /
101/2								

Step 6 To configure OSPF as the IGP in the core, you must simulate the provider core routers in the setup P1 as well as the PE Routers PE2, PE3, and PE4 as shown earlier in Figure 15-2.

To emulate the routers in the core, the first step is to highlight Port 101/2, which will simulate the OSPF network, and click **Add Session**. This will open the Session window where the parameters pertaining to core Router P1 in the topology can be added, as illustrated in Figure 15-24.

Step 7 In the Routing window, select the session just created under Port 101/2 and click the **Topology** button. This will open the OSPF Topology window, as shown in Figure 15-25. Note that the new router with router ID of 10.10.10.100 mapping to P1 is shown as a session router, which will be used to configure the rest of the OSPF.

Figure 15-24 *OSPF: LSA Configuration for MPLS Core*



101/1
2 6-ETH-IPV4 vlan:2 Disabled
101/2

Session: Port 101/2

Session Type: OSPF
# Sessions: 1
☐ Add to Sub-Interfaces

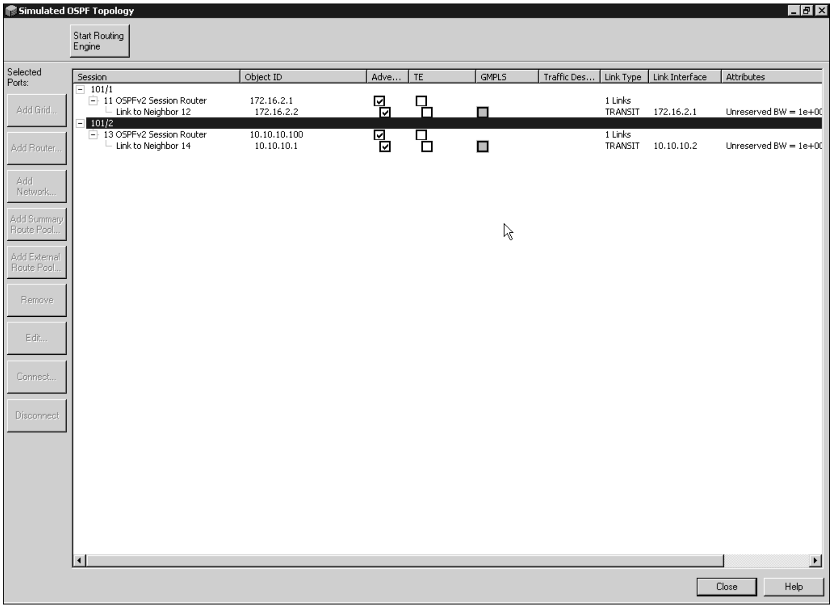
OSPF Version: OSPFv2
OSPF Network Type: Broadcast

Tester
Interface Address: 10 . 10 . 10 . 2 / 30 ☑ Auto Increment
Router ID: 10 . 10 . 10 . 100
Auto Increment applies to the Interface Address and Router ID.
Area ID: 0 . 0 . 0 . 0
Options: ☐ N-bit ☑ E-bit ☑ O-bit

SUT
Interface Address: 10 . 10 . 10 . 1 / 30 ☑ Auto Increment
Router ID: 10 . 10 . 10 . 101
Auto Increment applies only to the Interface Address.

GRE Tunneling
☐ Enable
Local: 10 . 10 . 10 . 2
Remote: 10 . 10 . 10 . 1
☑ Include Checksum Field

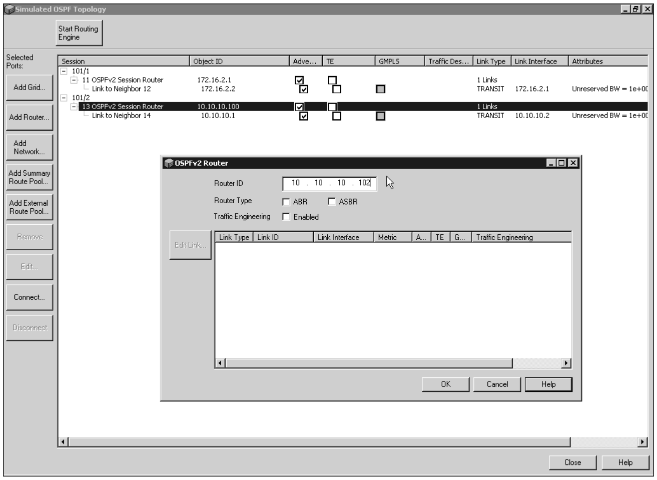
Figure 15-25 *OSPF: Topology Window*



Session	Object ID	Adve...	TE	GMPLS	Traffic Des...	Link Type	Link Interface	Attributes
101/1								
11 OSPFv2 Session Router	172.16.2.1	☑	☐			1 Links		
Link to Neighbor 12	172.16.2.2	☑	☐	▨		TRANSIT	172.16.2.1	Unreserved BW = 1e+00
101/2								
13 OSPFv2 Session Router	10.10.10.100	☑	☐			1 Links		
Link to Neighbor 14	10.10.10.1	☑	☐	▨		TRANSIT	10.10.10.2	Unreserved BW = 1e+00

Step 8 In the OSPF Topology window, select the **OSPFv2 Session Router 10.10.10.100** under Port 101/2 and select **Add Router**. This will open the OSPFv2 Router window where you can enter the router IDs of the three PE routers that you will have to emulate to repeat this process. The addition of Router PE2 is shown in Figure 15-26.

Figure 15-26 *OSPF: Topology Window: Add New Routers*



Session	Object ID	Adve...	TE	GMPLS	Traffic Des...	Link Type	Link Interface	Attributes
101/1								
11 OSPFv2 Session Router	172.16.2.1	☑	☐			1 Links		
Link to Neighbor 12	172.16.2.2	☑	☐	▨		TRANSIT	172.16.2.1	Unreserved BW = 1e+0C
101/2								
13 OSPFv2 Session Router	10.10.10.100	☑	☐			1 Links		
Link to Neighbor 14	10.10.10.1	☑	☐	▨		TRANSIT	10.10.10.2	Unreserved BW = 1e+0C

Router ID 10 . 10 . 10 . 102

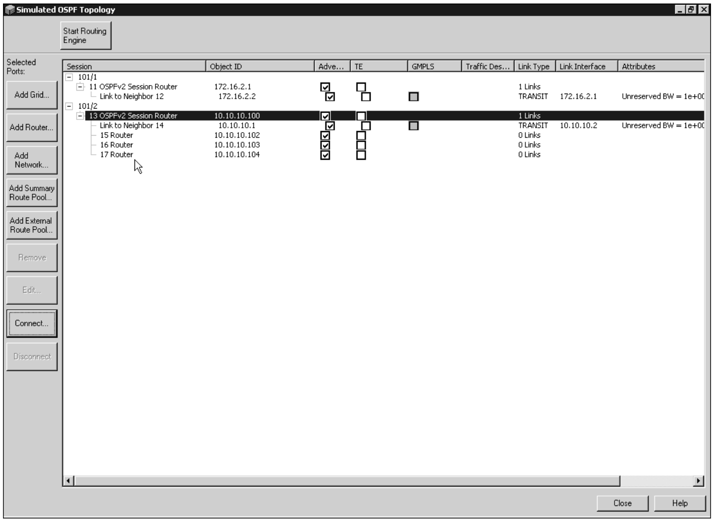
Router Type ☐ ABR ☐ ASBR

Traffic Engineering ☐ Enabled

Link Type	Link ID	Link Interface	Metric	A...	TE	G...	Traffic Engineering

Step 9 After repeating Step 8 for Routers PE3 and PE4, the Topology window will be populated by three new router entries, as depicted in Figure 15-27.

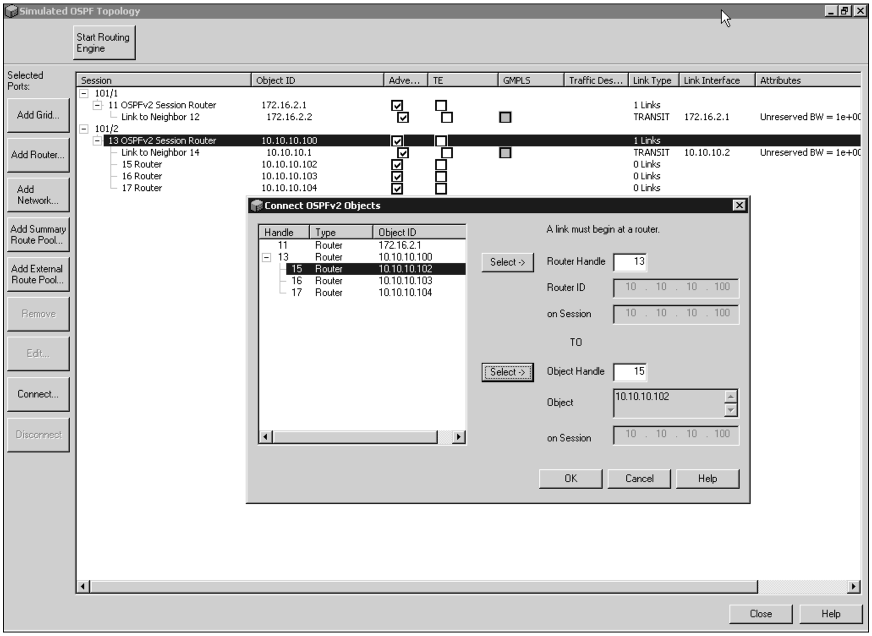
Figure 15-27 *OSPF: Topology Window with PE Routers*



Session	Object ID	Adve...	TE	GMPLS	Traffic Des...	Link Type	Link Interface	Attributes
101/1								
11 OSPFv2 Session Router	172.16.2.1	☑	☐			1 Links		
Link to Neighbor 12	172.16.2.2	☑	☐	▨		TRANSIT	172.16.2.1	Unreserved BW = 1e+0C
101/2								
13 OSPFv2 Session Router	10.10.10.100	☑	☐			1 Links		
Link to Neighbor 14	10.10.10.1	☑	☐	▨		TRANSIT	10.10.10.2	Unreserved BW = 1e+0C
15 Router	10.10.10.102	☑	☐			0 Links		
16 Router	10.10.10.103	☑	☐			0 Links		
17 Router	10.10.10.104	☑	☐			0 Links		

Step 10 Now, connect Router P1 (10.10.10.100) with Routers PE2, PE3, and PE4 that you created in Steps 8 and 9. To connect Routers P1 and PE2, select the **OSPFv2 Session Router 10.10.10.100** under Port 101/2 and select **Connect**. This will open the Connect OSPFv2 Objects window, as shown in Figure 15-28. Select the **router session** in the Connect OSPFv2 Objects window mapping to PE2 (10.10.10.102) and click **Select** next to the Object Handle and click **OK**.

Figure 15-28 *OSPF Topology: Link Addition*



Session	Object ID	Adve...	TE	GMPLS	Traffic Des...	Link Type	Link Interface	Attributes
101/1								
11 OSPFv2 Session Router	172.16.2.1	☑	☐			1 Links		
Link to Neighbor 12	172.16.2.2	☑	☐	▨		TRANSIT	172.16.2.1	Unreserved BW = 1e+0
101/2								
13 OSPFv2 Session Router	10.10.10.100	☑	☐			1 Links		
Link to Neighbor 14	10.10.10.1	☑	☐	▨		TRANSIT	10.10.10.2	Unreserved BW = 1e+0
15 Router	10.10.10.102	☑	☐			0 Links		
16 Router	10.10.10.103	☑	☐			0 Links		
17 Router	10.10.10.104	☑	☐			0 Links		

Handle	Type	Object ID
11	Router	172.16.2.1
13	Router	10.10.10.100
15	Router	10.10.10.102
16	Router	10.10.10.103
17	Router	10.10.10.104

A link must begin at a router.

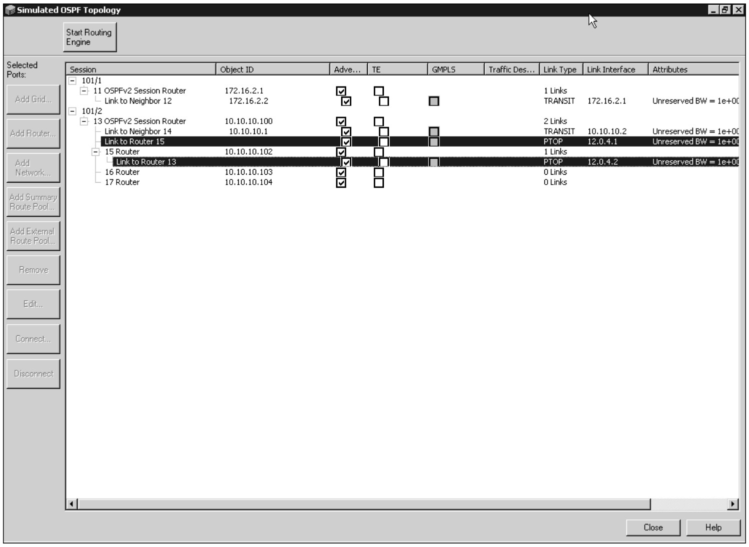
Router Handle: 13
Router ID: 10 . 10 . 10 . 100
on Session: 10 . 10 . 10 . 100

TO

Object Handle: 15
Object: 10.10.10.102
on Session: 10 . 10 . 10 . 100

Step 11 This creates a point-to-point link between the session router 10.10.10.100 and the PE2 router 10.10.10.l02, as illustrated in the highlighted rows in Figure 15-29.

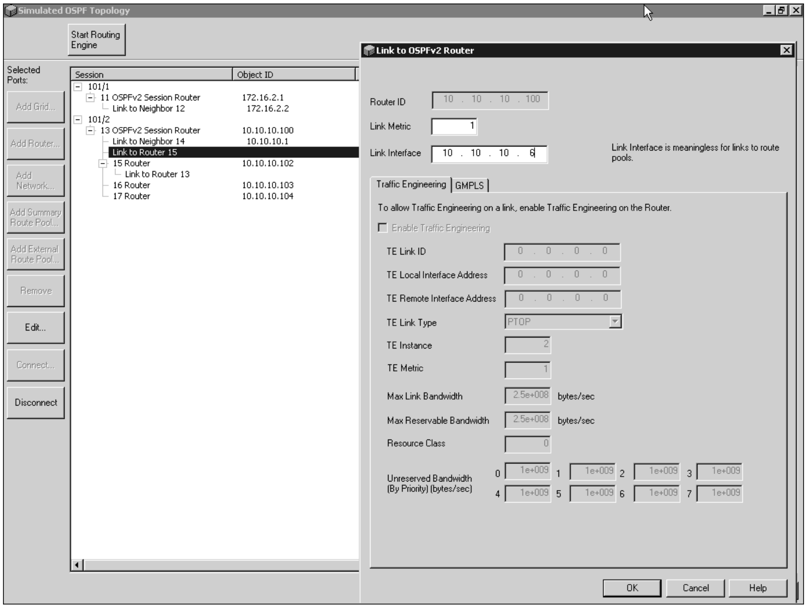
Figure 15-29 *OSPF Topology: New Links in Topology Window*



Session	Object ID	Adve...	TE	GMPLS	Traffic Des...	Link Type	Link Interface	Attributes
101/1								
11 OSPFv2 Session Router	172.16.2.1	☑	☐			1 Links		
Link to Neighbor 12	172.16.2.2	☑	☐	▨		TRANSIT	172.16.2.1	Unreserved BW = 1e+00
101/2								
13 OSPFv2 Session Router	10.10.10.100	☑	☐			2 Links		
Link to Neighbor 14	10.10.10.1	☑	☐	▨		TRANSIT	10.10.10.2	Unreserved BW = 1e+00
Link to Router 15		☑	☐	▨		PTOP	12.0.4.1	Unreserved BW = 1e+00
15 Router	10.10.10.102	☑	☐			1 Links		
Link to Router 13		☑	☐	▨		PTOP	12.0.4.2	Unreserved BW = 1e+00
16 Router	10.10.10.103	☑	☐			0 Links		
17 Router	10.10.10.104	☑	☐			0 Links		

Step 12 Highlight the link that you want to edit in the Topology window and click the **Edit** button. This opens the Link to OSPFv2 Router window where you can change the IP address on the router pertaining to the link, as illustrated in Figure 15-30.

Figure 15-30 *OSPF Topology: Changing Link IP*



Session	Object ID
101/1	
11 OSPFv2 Session Router	172.16.2.1
Link to Neighbor 12	172.16.2.2
101/2	
13 OSPFv2 Session Router	10.10.10.100
Link to Neighbor 14	10.10.10.1
Link to Router 15	
15 Router	10.10.10.102
Link to Router 13	
16 Router	10.10.10.103
17 Router	10.10.10.104

Router ID 10 . 10 . 10 . 100

Link Metric 1

Link Interface 10 . 10 . 10 . 6

Link Interface is meaningless for links to route pools.

To allow Traffic Engineering on a link, enable Traffic Engineering on the Router.

☐ Enable Traffic Engineering

TE Link ID 0 . 0 . 0 . 0

TE Local Interface Address 0 . 0 . 0 . 0

TE Remote Interface Address 0 . 0 . 0 . 0

TE Link Type PTOP

TE Instance 2

TE Metric 1

Max Link Bandwidth 2.5e+008 bytes/sec

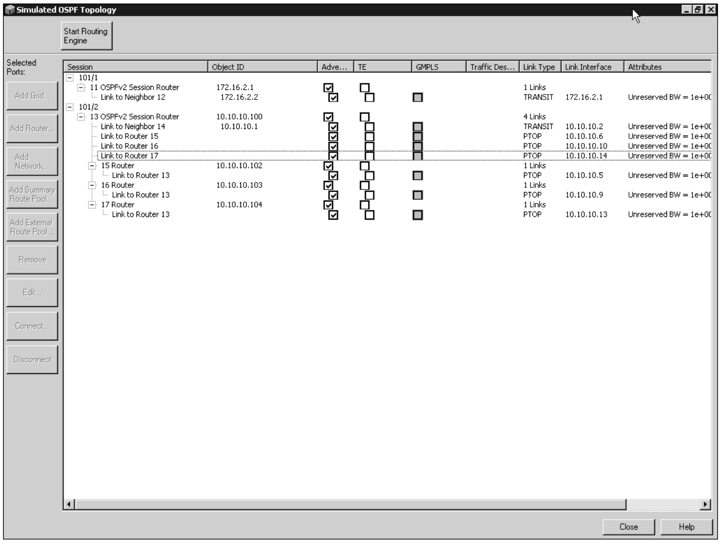
Max Reservable Bandwidth 2.5e+008 bytes/sec

Resource Class 0

Unreserved Bandwidth (By Priority) (bytes/sec) 0 1e+009 1 1e+009 2 1e+009 3 1e+009
4 1e+009 5 1e+009 6 1e+009 7 1e+009

Step 13 Repeat Steps 10 through 12 for Routers PE3 and PE4 to arrive at the topology shown in Figure 15-31.

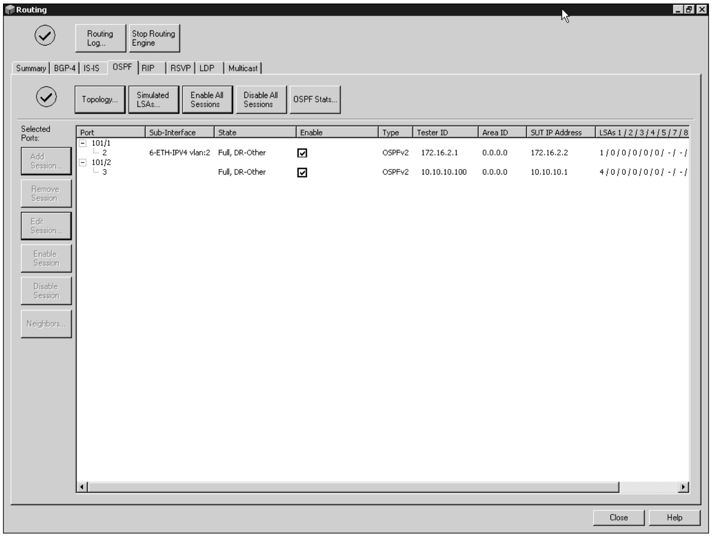
Figure 15-31 *OSPF Topology: Complete*



Session	Object ID	Adve...	TE	GMPLS	Traffic Des...	Link Type	Link Interface	Attributes
101/1								
11 OSPFv2 Session Router	172.16.2.1	☑	☐			1 Links		
Link to Neighbor 12	172.16.2.2	☑	☐	▨		TRANSIT	172.16.2.1	Unreserved BW = 1e+00
101/2								
13 OSPFv2 Session Router	10.10.10.100	☑	☐			4 Links		
Link to Neighbor 14	10.10.10.1	☑	☐	▨		TRANSIT	10.10.10.2	Unreserved BW = 1e+00
Link to Router 15		☑	☐	▨		PTOP	10.10.10.6	Unreserved BW = 1e+00
Link to Router 16		☑	☐	▨		PTOP	10.10.10.10	Unreserved BW = 1e+00
Link to Router 17		☑	☐	▨		PTOP	10.10.10.14	Unreserved BW = 1e+00
15 Router	10.10.10.102	☑	☐			1 Links		
Link to Router 13		☑	☐	▨		PTOP	10.10.10.5	Unreserved BW = 1e+00
16 Router	10.10.10.103	☑	☐			1 Links		
Link to Router 13		☑	☐	▨		PTOP	10.10.10.9	Unreserved BW = 1e+00
17 Router	10.10.10.104	☑	☐			1 Links		
Link to Router 13		☑	☐	▨		PTOP	10.10.10.13	Unreserved BW = 1e+00

Step 14 Close the Topology window to return to the Routing window. Enable all sessions by clicking the **Enable All Sessions** button. Click **Start Routing Engine**. The state must go from Disabled to Full, as shown in Figure 15-32.

Figure 15-32 *OSPF PE-CE and IGP Configuration*



Port	Sub-Interface	State	Enable	Type	Tester ID	Area ID	SUT IP Address	LSAs 1 / 2 / 3 / 4 / 5 / 7 / 8
101/1								
2	6-ETH-IPV4 vlan:2	Full, DR-Other	☑	OSPFv2	172.16.2.1	0.0.0.0	172.16.2.2	1 / 0 / 0 / 0 / 0 / 0 / - / - /
101/2								
3		Full, DR-Other	☑	OSPFv2	10.10.10.100	0.0.0.0	10.10.10.1	4 / 0 / 0 / 0 / 0 / 0 / - / - /

Step 15 Verification of DUT reception of OSPF and operation is shown in Example 15-3.

Example 15-3 *DUT Verification OSPF PE-CE and OSPF IGP*

```
DUT#show ip route vrf vpn2 ospf
Routing Table: vpn2
O    192.168.31.0/24 [110/2] via 172.16.2.1, 00:00:12, GigabitEthernet0/1.2
O    192.168.30.0/24 [110/2] via 172.16.2.1, 00:00:12, GigabitEthernet0/1.2
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O    172.16.2.1/32 [110/1] via 172.16.2.1, 00:00:12, GigabitEthernet0/1.2
DUT#show ip route ospf
     10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
O       10.10.10.8/30 [110/2] via 10.10.10.2, 00:00:16, GigabitEthernet0/2
O       10.10.10.12/30 [110/2] via 10.10.10.2, 00:00:16, GigabitEthernet0/2
O       10.10.10.4/30 [110/2] via 10.10.10.2, 00:00:16, GigabitEthernet0/2
O       10.10.10.104/32 [110/2] via 10.10.10.2, 00:00:16, GigabitEthernet0/2
O       10.10.10.102/32 [110/2] via 10.10.10.2, 00:00:16, GigabitEthernet0/2
O       10.10.10.103/32 [110/2] via 10.10.10.2, 00:00:16, GigabitEthernet0/2
O       10.10.10.100/32 [110/1] via 10.10.10.2, 00:00:16, GigabitEthernet0/2
```

N2X BGP PE-CE and MP-BGP Configuration

The following steps illustrate the implementation of BGP PE-CE between the DUT and the emulated CE3 router:

Step 1 Click the **BGP-4** tab on the Routing window.

(a) Highlight **Port 101/1** in the window and click **Add BGP-4 session**.

(b) This will open the Session window for Port 101/1.

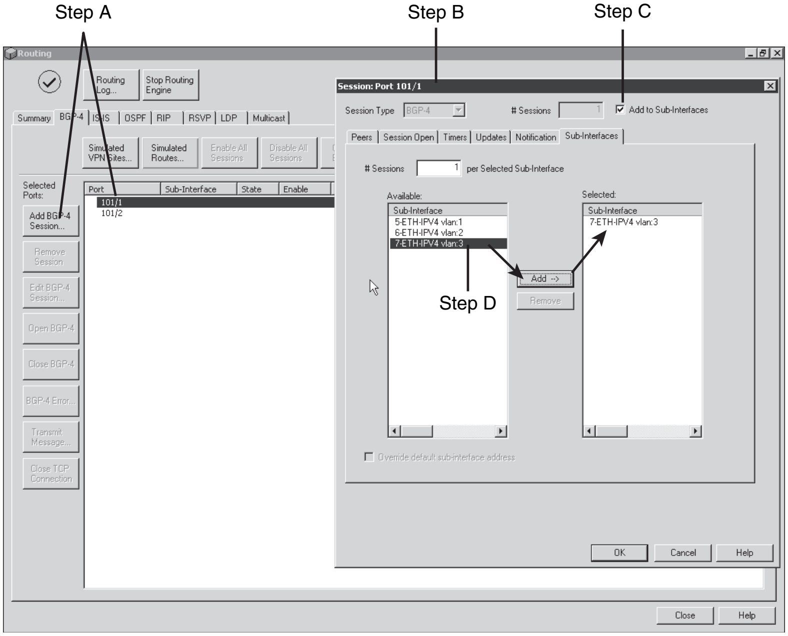
(c) In the Session window, check mark **Add to Sub-Interfaces**, which will automatically take you to the Sub-Interfaces tab.

(d) Select **5-ETH-IPV4 vlan:3**, which is the sub-interface mapping to the CE3 connection in the Available Sub-Interfaces window, and click **Add** to add the same to the selected sub-interfaces, as shown in Figure 15-33.

Step 2 Configure the routes to be generated by selecting the session in the Routing window and clicking the **Simulated Routes** button. In the Simulated Routes window, highlight the **IPv4** tab under the PE-CE session and click **Add Route Pools**. Select **Single Route Pool** and enter the appropriate IP address ranges as required by the setup. This is illustrated in Figure 15-34.

Click **OK** and then **Close** to close the Simulated Routes window.

Figure 15-33 *BGP: Add Session on 101/1*



101/1
101/2

Session Type: BGP-4
Sessions: 1
☑ Add to Sub-Interfaces

Sessions: 1 per Selected Sub-Interface

Available:

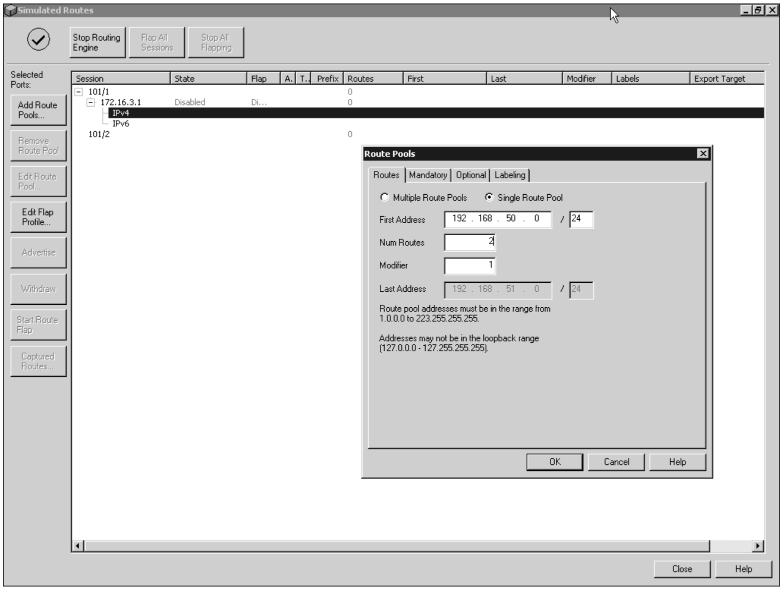
Sub-Interface
5-ETH-IPV4 vlan:1
6-ETH-IPV4 vlan:2
7-ETH-IPV4 vlan:3

Selected:

Sub-Interface
7-ETH-IPV4 vlan:3

☐ Override default sub-interface address

Figure 15-34 *BGP Route Addition on CE Session*



Session	State	Flap	A.	T.	Prefix	Routes	First	Last	Modifier	Labels	Export Target
101/1						0					
172.16.3.1	Disabled	Di...				0					
IPv4											
IPv6											
101/2						0					

○ Multiple Route Pools ● Single Route Pool

First Address: 192 . 168 . 50 . 0 / 24

Num Routes: 2

Modifier: 1

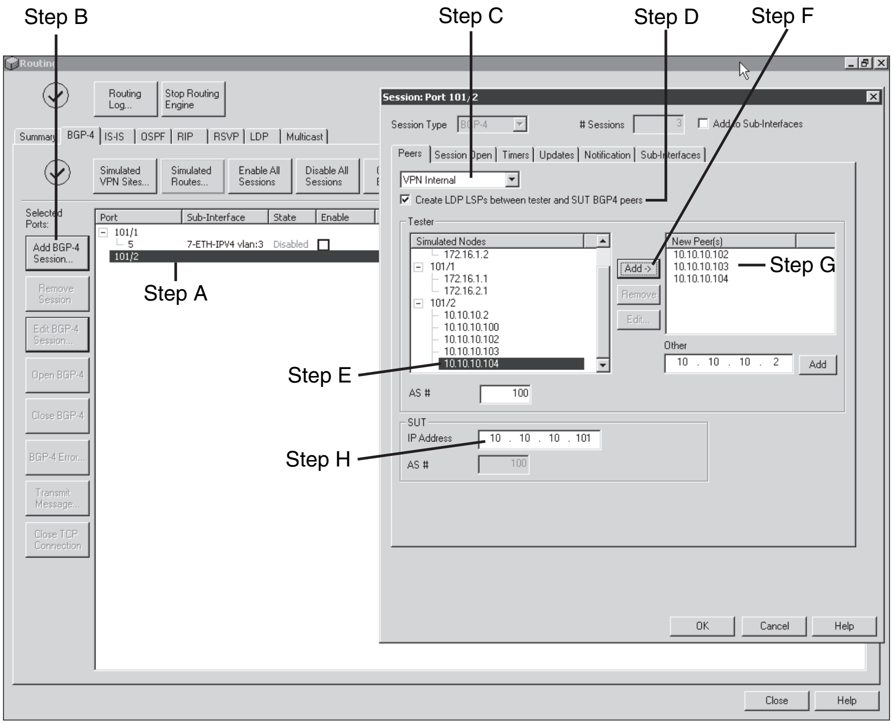
Last Address: 192 . 168 . 51 . 0 / 24

Route pool addresses must be in the range from 1.0.0.0 to 223.255.255.255.

Addresses may not be in the loopback range (127.0.0.0 - 127.255.255.255).

Step 3 The configuration for MP-iBGP peer addition is shown in Figure 15-35 and is performed as follows:

Figure 15-35 *MP-iBGP Peer Addition*



Session: Port 101/2

Session Type: BGP-4

Sessions: 3

☐ Add to Sub-Interfaces

VPN Internal

☑ Create LDP LSPs between tester and SUT BGP4 peers

Tester

Simulated Nodes:
- 172.16.1.2
- 101/1
  - 172.16.1.1
  - 172.16.2.1
- 101/2
  - 10.10.10.2
  - 10.10.10.100
  - 10.10.10.102
  - 10.10.10.103
  - 10.10.10.104

New Peer(s):
- 10.10.10.102
- 10.10.10.103
- 10.10.10.104

Other: 10 . 10 . 10 . 2

AS #: 100

SUT

IP Address: 10 . 10 . 10 . 101

AS #: 100

Port	Sub-Interface	State	Enable
101/1			
5	7-ETH-IPV4 vlan:3	Disabled	☐
101/2			

(a) Click **Port 101/2** to configure the core MP-iBGP sessions.

(b) Click the **Add BGP-4 Session** button to open the Session window.

(c) In the Session window under the **Peers** tab, select peer type to **VPN Internal**.

(d) Select the **Create LDP LSPs between tester and SUT BGP4 peers** option. This automatically creates LDP LSPs along with the BGP peering.

(e) Select the loopback addresses mapping to the PE routers in the Simulated Nodes window.

(f) Click **Add** to add the peers to the New Peers window.

(g) Repeat for all PE loopback addresses.

(h) Change the IP address of the SUT to map to the loopback address on the SUT 10.10.10.101.

(i) Click **OK** to close the Session window.

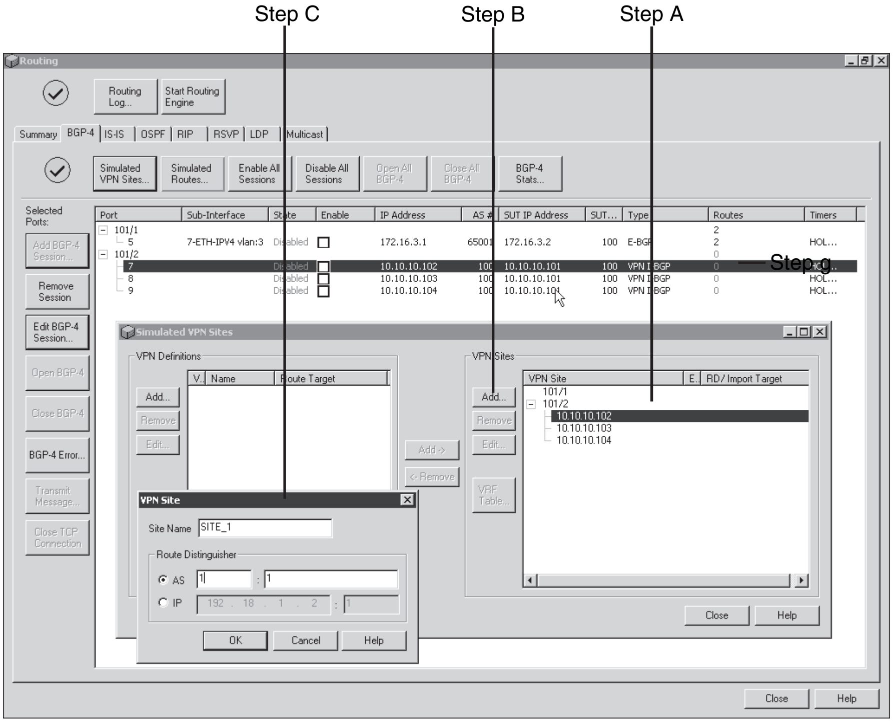
Step 4 Click the **Simulated VPN Sites** button in the Routing window.

(a) Highlight the remote PE loopback address in the VPN Site window.

(b) Click **Add** to open the VPN Site dialog box.

(c) Configure the RD values mapping to that site. Figure 15-36 shows the configuration of RD value of 1:1 for Site_1 on 10.10.10.102 (PE2).

Figure 15-36 *MP-iBGP Peer RD Configuration*



Port	Sub-Interface	State	Enable	IP Address	AS #	SUT IP Address	SUT...	Type	Routes	Timers
101/1									2	
5	7-ETH-IPV4 vlan:3	Disabled	☐	172.16.3.1	65001	172.16.3.2	100	E-BGP	2	HOL...
101/2									0	
7		Disabled	☐	10.10.10.102	100	10.10.10.101	100	VPN I-BGP	0	HOL...
8		Disabled	☐	10.10.10.103	100	10.10.10.101	100	VPN I-BGP	0	HOL...
9		Disabled	☐	10.10.10.104	100	10.10.10.101	100	VPN I-BGP	0	HOL...

V.	Name	Route Target

VPN Site	E.	RD/ Import Target
101/1		
101/2		
10.10.10.102		
10.10.10.103		
10.10.10.104		

VPN Site

Site Name: SITE_1

Route Distinguisher

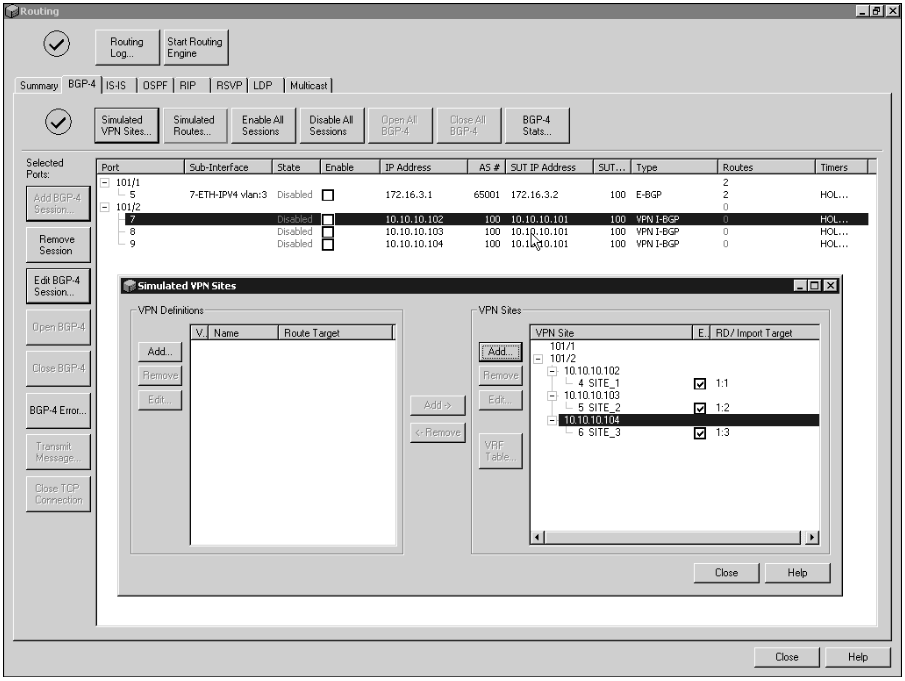
● AS 1 : 1

○ IP 192 . 18 . 1 . 2 : 1

OK Cancel Help

Repeat Steps 4a through 4c for all PE routers to add Site_1, Site_2, and Site_3 on PE2, PE3, and PE4 with RD 1:1, 1:2, and 1:3, respectively, as shown in Figure 15-37.

Figure 15-37 *MP-iBGP Peer Site Configuration*



Port	Sub-Interface	State	Enable	IP Address	AS #	SUT IP Address	SUT...	Type	Routes	Timers
⊟ 101/1									2	
5	7-ETH-IPV4 vlan:3	Disabled	☐	172.16.3.1	65001	172.16.3.2	100	E-BGP	2	HOL...
⊟ 101/2									0	
7		Disabled	☐	10.10.10.102	100	10.10.10.101	100	VPN I-BGP	0	HOL...
8		Disabled	☐	10.10.10.103	100	10.10.10.101	100	VPN I-BGP	0	HOL...
9		Disabled	☐	10.10.10.104	100	10.1[illegible]10.101	100	VPN I-BGP	0	HOL...

V..	Name	Route Target

VPN Site	E..	RD/ Import Target
101/1		
⊟ 101/2		
⊟ 10.10.10.102		
4 SITE_1	☑	1:1
⊟ 10.10.10.103		
5 SITE_2	☑	1:2
⊟ 10.10.10.104		
6 SITE_3	☑	1:3

Step 5 Click **Close** to close the Simulated VPN Sites window.

(a) Click the **Simulated Routes** button in the Routing window.

(b) Highlight the **Site_1** session under Port 101/2 for peer 10.10.10.102.

(c) Click **Add Route Pools**. This opens the Route Pools configuration window.

(d) Select **Single Route Pool**.

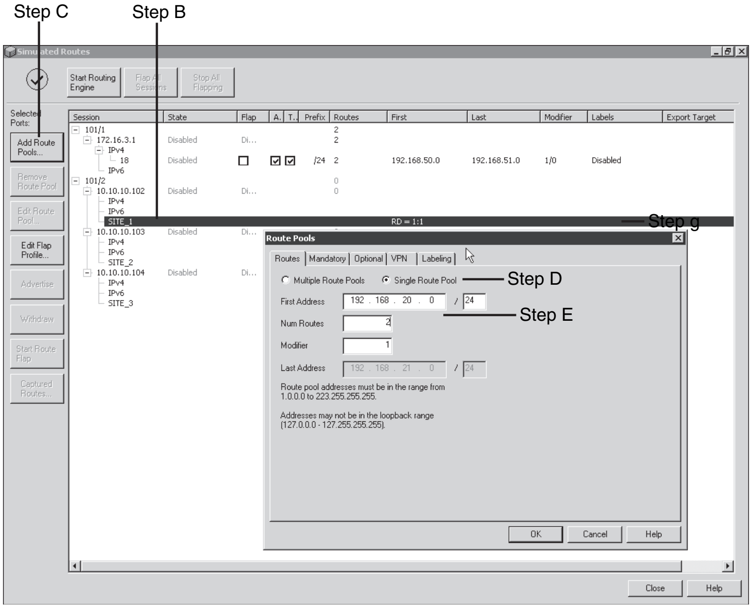
(e) Enter appropriate values into the Route Pool configuration window to generate prefixes 192.168.20.0 and 192.168.21.0, as shown in Figure 15-38.

(f) Select the **VPN** tab under the Route Pool configuration window, as shown in Figure 15-39.

(g) Configure the appropriate export route target mapping to the prefixes generated in the window.

(h) Click **OK** to close.

Figure 15-38 *Configuring MP-iBGP Routes*



Session	State	Flap	A.	T.	Prefix	Routes	First	Last	Modifier	Labels	Export Target
101/1						2					
172.16.3.1	Disabled	Di...				2					
IPv4											
18	Disabled	☐	☑	☑	/24	2	192.168.50.0	192.168.51.0	1/0	Disabled	
IPv6											
101/2						0					
10.10.10.102	Disabled	Di...				0					
IPv4											
IPv6											
SITE_1							RD = 1:1				
10.10.10.103	Disabled	Di...									
IPv4											
IPv6											
SITE_2											
10.10.10.104	Disabled	Di...									
IPv4											
IPv6											
SITE_3											

○ Multiple Route Pools ● Single Route Pool

First Address: 192 . 168 . 20 . 0 / 24

Num Routes: 2

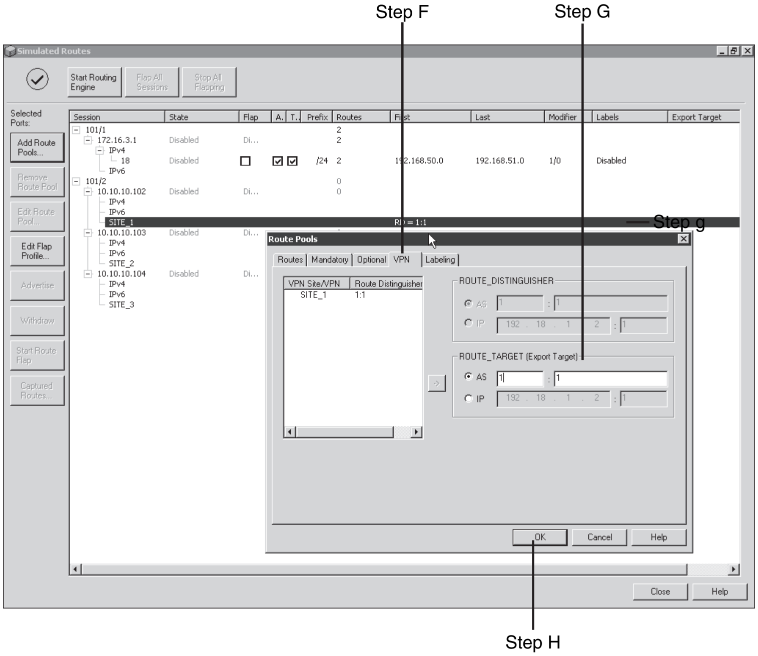
Modifier: 1

Last Address: 192 . 168 . 21 . 0 / 24

Route pool addresses must be in the range from 1.0.0.0 to 223.255.255.255.

Addresses may not be in the loopback range (127.0.0.0 - 127.255.255.255).

Figure 15-39 *Configuring MP-iBGP Routes: Export Route Targets*



Session	State	Flap	A.	T.	Prefix	Routes	First	Last	Modifier	Labels	Export Target
101/1						2					
172.16.3.1	Disabled	Di...				2					
IPv4											
18	Disabled	☐	☑	☑	/24	2	192.168.50.0	192.168.51.0	1/0	Disabled	
IPv6											
101/2						0					
10.10.10.102	Disabled	Di...				0					
IPv4											
IPv6											
SITE_1							RD = 1:1				
10.10.10.103	Disabled	Di...									
IPv4											
IPv6											
SITE_2											
10.10.10.104	Disabled	Di...									
IPv4											
IPv6											
SITE_3											

VPN Site/VPN	Route Distinguisher
SITE_1	1:1

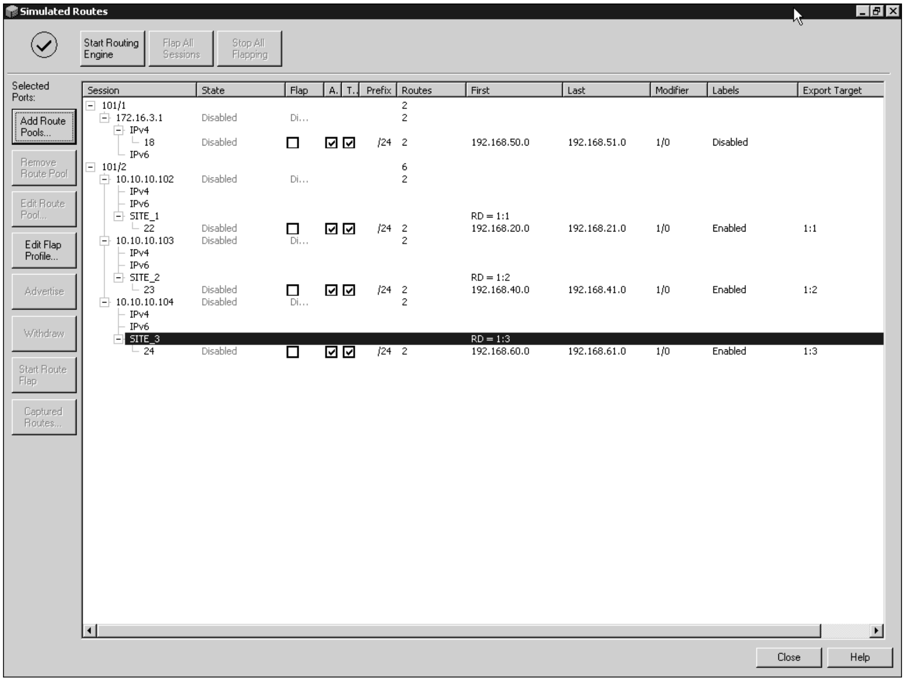
ROUTE_DISTINGUISHER
● AS 1 : 1
○ IP 192 . 18 . 1 . 2 : 1

ROUTE_TARGET (Export Target)
● AS 1 : 1
○ IP 192 . 18 . 1 . 2 : 1

Step 6 Repeat all steps in Step 5 for the other PE routers and associated prefixes.

Step 7 The final configuration on the Simulated Routes window is shown in Figure 15-40.

Figure 15-40 *Simulated Routes*



Session	State	Flap	A.	T..	Prefix	Routes	First	Last	Modifier	Labels	Export Target
101/1						2					
172.16.3.1	Disabled	Di...				2					
IPv4											
18	Disabled	☐	☑	☑	/24	2	192.168.50.0	192.168.51.0	1/0	Disabled	
IPv6											
101/2						6					
10.10.10.102	Disabled	Di...				2					
IPv4											
IPv6											
SITE_1							RD = 1:1				
22	Disabled	☐	☑	☑	/24	2	192.168.20.0	192.168.21.0	1/0	Enabled	1:1
10.10.10.103	Disabled	Di...				2					
IPv4											
IPv6											
SITE_2							RD = 1:2				
23	Disabled	☐	☑	☑	/24	2	192.168.40.0	192.168.41.0	1/0	Enabled	1:2
10.10.10.104	Disabled	Di...				2					
IPv4											
IPv6											
SITE_3							RD = 1:3				
24	Disabled	☐	☑	☑	/24	2	192.168.60.0	192.168.61.0	1/0	Enabled	1:3

Step 8 Click **Close** to close the Simulated Routes window and click **Enable All Sessions** in the Routing window followed by **Start Routing Engine**.

Step 9 Verify the operation of BGP PE-CE as well as MP-iBGP on the DUT, as shown in Example 15-4.

Example 15-4 *DUT Verification of BGP PE-CE and MP-iBGP*

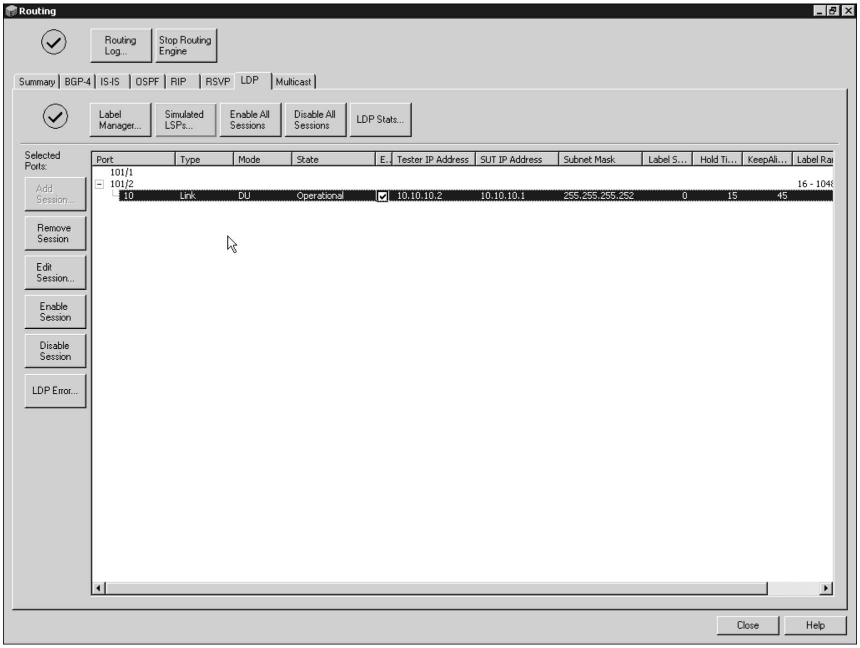
```
DUT#show ip route vrf vpn1 bgp
B    192.168.21.0/24 [200/0] via 10.10.10.102, 00:03:00
B    192.168.20.0/24 [200/0] via 10.10.10.102, 00:03:00
DUT#show ip route vrf vpn2 bgp
B    192.168.40.0/24 [200/0] via 10.10.10.103, 00:03:05
B    192.168.41.0/24 [200/0] via 10.10.10.103, 00:03:05
DUT#show ip route vrf vpn3 bgp
B    192.168.61.0/24 [200/0] via 10.10.10.104, 00:03:24
B    192.168.60.0/24 [200/0] via 10.10.10.104, 00:03:24
B    192.168.51.0/24 [20/0] via 172.16.3.1, 00:01:00
B    192.168.50.0/24 [20/0] via 172.16.3.1, 00:01:00
```

N2X LDP Configuration

To configure LDP, click the **LDP** tab in the Routing window. Because LDP has already been configured as a result of the MP-iBGP configuration, you only need to enable the same by clicking on the **Enable All Sessions** button.

The LDP state will then go from Disabled to Operational, as shown in Figure 15-41.

Figure 15-41 *LDP Session Operational*



Port	Type	Mode	State	E..	Tester IP Address	SUT IP Address	Subnet Mask	Label S...	Hold Ti...	KeepAli...	Label Ra
101/1											
101/2											16 - 104
10	Link	DU	Operational	☑	10.10.10.2	10.10.10.1	255.255.255.252	0	15	45	

Verify LDP neighbor relationship and label exchange by performing the appropriate commands on the DUT, as shown in Example 15-5.

Example 15-5 *DUT Verification LDP*

```
DUT#show mpls ldp neighbor
    Peer LDP Ident: 10.10.10.2:0; Local LDP Ident 10.10.10.101:0
        TCP connection: 10.10.10.2.646 - 10.10.10.101.32222
        State: Oper; Msgs sent/rcvd: 34/29; Downstream
        Up time: 00:04:58
        LDP discovery sources:
          GigabitEthernet0/2, Src IP addr: 10.10.10.2
        Addresses bound to peer LDP Ident:
          10.10.10.2

DUT#show mpls ldp bindings
  tib entry: 10.10.10.0/30, rev 61
        local binding:  tag: imp-null
```

continues

Example 15-5 *DUT Verification LDP (Continued)*

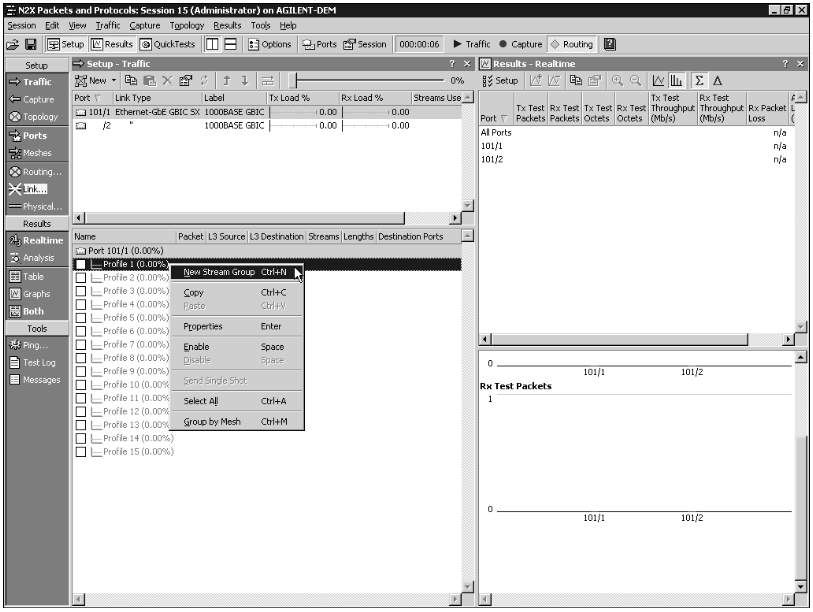
```
tib entry: 10.10.10.4/30, rev 84
      local binding:  tag: 23
tib entry: 10.10.10.8/30, rev 86
      local binding:  tag: 24
tib entry: 10.10.10.12/30, rev 88
      local binding:  tag: 25
tib entry: 10.10.10.100/32, rev 90
      local binding:  tag: 26
tib entry: 10.10.10.101/32, rev 4
      local binding:  tag: imp-null
tib entry: 10.10.10.102/32, rev 92
      local binding:  tag: 27
tib entry: 10.10.10.103/32, rev 94
      local binding:  tag: 28
tib entry: 10.10.10.104/32, rev 96
      local binding:  tag: 29
```

N2X MPLS Traffic Generation

In this section, you generate a traffic stream from the local CE routes to the remote PE generated VPNv4 routes and verify operation:

Step 1 Highlight **Port 101/1** in the Setup-Traffic pane and, in the Traffic Profiles pane, right-click the first profile and select **New Stream Group**, as shown in Figure 15-42.

Figure 15-42 *Adding a New Stream Group*



N2X Packets and Protocols: Session 15 (Administrator) on AGILENT-DEM

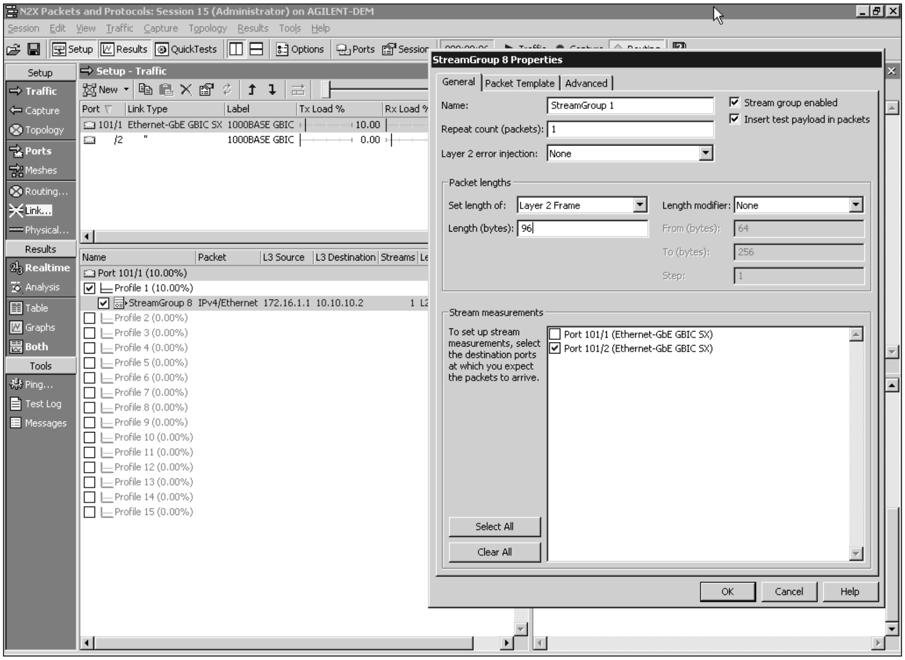
Port	Link Type	Label	Tx Load %	Rx Load %	Streams Use
101/1	Ethernet-GbE GBIC SX	1000BASE GBIC	0.00	0.00	
/2	"	1000BASE GBIC	0.00	0.00	

Name	Packet	L3 Source	L3 Destination	Streams	Lengths	Destination Ports
Port 101/1 (0.00%)						
☐ Profile 1 (0.00%)						
☐ Profile 2 (0.00%)						
☐ Profile 3 (0.00%)						
☐ Profile 4 (0.00%)						
☐ Profile 5 (0.00%)						
☐ Profile 6 (0.00%)						
☐ Profile 7 (0.00%)						
☐ Profile 8 (0.00%)						
☐ Profile 9 (0.00%)						
☐ Profile 10 (0.00%						
☐ Profile 11 (0.00%						
☐ Profile 12 (0.00%						
☐ Profile 13 (0.00%						
☐ Profile 14 (0.00%)						
☐ Profile 15 (0.00%)						

Port	Tx Test Packets	Rx Test Packets	Tx Test Octets	Rx Test Octets	Tx Test Throughput (Mb/s)	Rx Test Throughput (Mb/s)	Rx Packet Loss
All Ports							n/a
101/1							n/a
101/2							n/a

Step 2 Step 1 will create a new stream group under the selected profile. Double-click the stream group to open the properties for the stream group. Under the General tab in the StreamGroup 8 Properties window, change the properties, as shown in Figure 15-43. Also, make sure Port 101/2 is identified as a valid traffic destination.

Figure 15-43 *Stream Group Configuration-1*



Port	Link Type	Label	Tx Load %
101/1	Ethernet-GbE GBIC SX	1000BASE GBIC	10.00
/2	"	1000BASE GBIC	0.00

Name	Packet	L3 Source	L3 Destination	Streams
Port 101/1 (10.00%)				
☑ Profile 1 (10.00%)				
☑ StreamGroup 8	IPv4/Ethernet	172.16.1.1	10.10.10.2	1
☐ Profile 2 (0.00%)				
☐ Profile 3 (0.00%)				
☐ Profile 4 (0.00%)				
☐ Profile 5 (0.00%)				
☐ Profile 6 (0.00%)				
☐ Profile 7 (0.00%)				
☐ Profile 8 (0.00%)				
☐ Profile 9 (0.00%)				
☐ Profile 10 (0.00%)				
☐ Profile 11 (0.00%)				
☐ Profile 12 (0.00%)				
☐ Profile 13 (0.00%)				
☐ Profile 14 (0.00%)				
☐ Profile 15 (0.00%)				

Name: StreamGroup 1
Repeat count (packets): 1
Layer 2 error injection: None
☑ Stream group enabled
☑ Insert test payload in packets

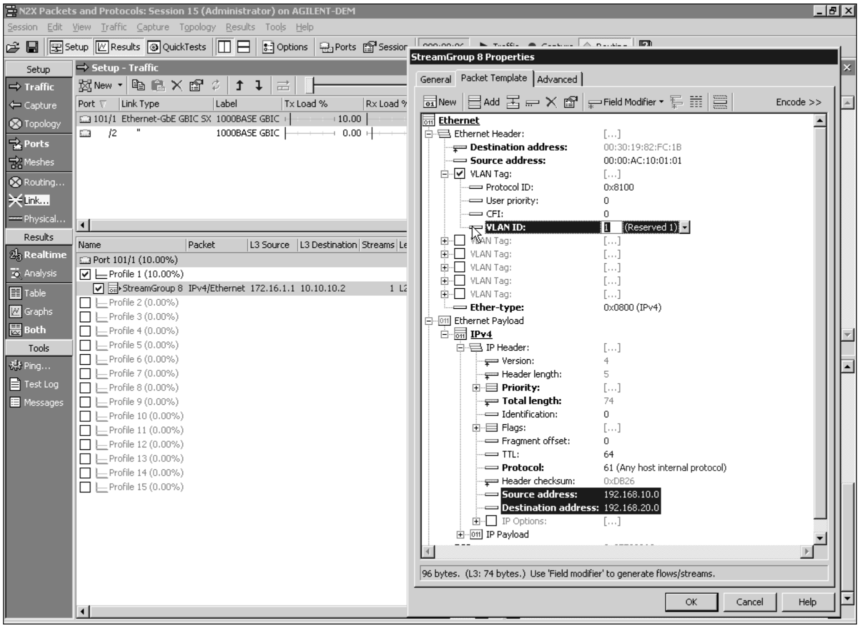
Packet lengths
Set length of: Layer 2 Frame
Length (bytes): 96
Length modifier: None
From (bytes): 64
To (bytes): 256
Step: 1

Stream measurements
To set up stream measurements, select the destination ports at which you expect the packets to arrive.
☐ Port 101/1 (Ethernet-GbE GBIC SX)
☑ Port 101/2 (Ethernet-GbE GBIC SX)

Step 3 Under the Packet Template tab, expand the VLAN header and the IPv4 header, and configure the appropriate VLAN ID and source and destination addresses for the prefixes mapping to the VPN1 source and destinations shown in Figure 15-44. Click **OK** to close the StreamGroup 8 Properties window.

Step 4 Repeat Steps 1 through 3 to create two more streams for VPN prefixes mapping to VPN2 and VPN3, as shown in Figure 15-45. Finally, click the **Traffic** button in the toolbar to start the traffic.

Figure 15-44 *Stream Group Configuration-2*



N2X Packets and Protocols: Session 15 (Administrator) on AGILENT-DEM

Setup - Traffic

Port	Link Type	Label	Tx Load %	Rx Load %
101/1	Ethernet-GbE GBIC SX	1000BASE GBIC	10.00	
/2	"	1000BASE GBIC	0.00	

Name	Packet	L3 Source	L3 Destination	Streams
Port 101/1 (10.00%)				
☑ Profile 1 (10.00%)				
☑ StreamGroup 8	IPv4/Ethernet	172.16.1.1	10.10.10.2	1
☐ Profile 2 (0.00%)				
☐ Profile 3 (0.00%)				
☐ Profile 4 (0.00%)				
☐ Profile 5 (0.00%)				
☐ Profile 6 (0.00%)				
☐ Profile 7 (0.00%)				
☐ Profile 8 (0.00%)				
☐ Profile 9 (0.00%)				
☐ Profile 10 (0.00%)				
☐ Profile 11 (0.00%)				
☐ Profile 12 (0.00%)				
☐ Profile 13 (0.00%)				
☐ Profile 14 (0.00%)				
☐ Profile 15 (0.00%)				

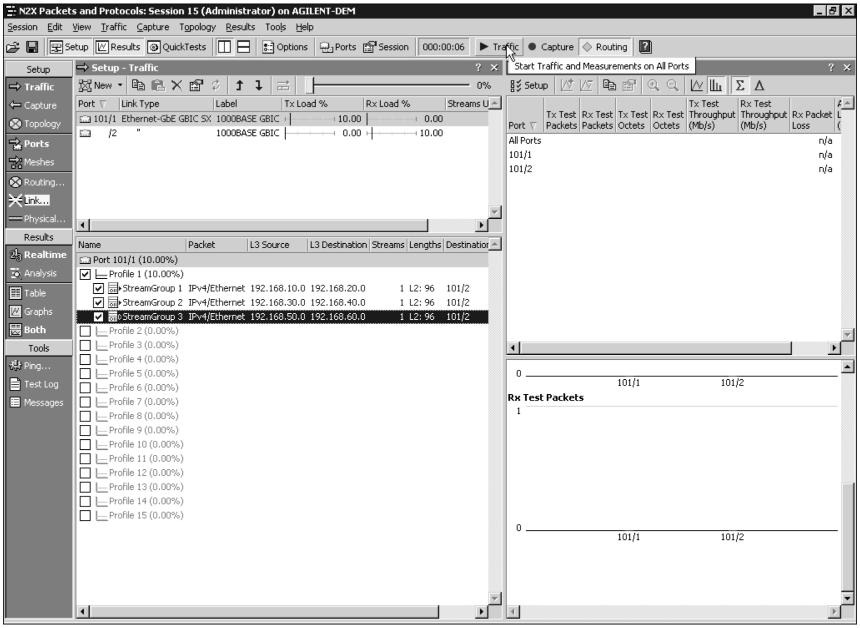
StreamGroup 8 Properties

Packet Template

```
Ethernet
  Ethernet Header:            [...]
    Destination address:      00:30:19:82:FC:1B
    Source address:           00:00:AC:10:01:01
    ☑ VLAN Tag:               [...]
      Protocol ID:            0x8100
      User priority:          0
      CFI:                    0
      VLAN ID:                1 (Reserved 1)
    ☐ VLAN Tag:               [...]
    ☐ VLAN Tag:               [...]
    ☐ VLAN Tag:               [...]
    ☐ VLAN Tag:               [...]
    ☐ VLAN Tag:               [...]
    Ether-type:               0x0800 (IPv4)
  Ethernet Payload
    IPv4
      IP Header:              [...]
        Version:              4
        Header length:        5
        Priority:             [...]
        Total length:         74
        Identification:       0
        Flags:                [...]
        Fragment offset:      0
        TTL:                  64
        Protocol:             61 (Any host internal protocol)
        Header checksum:      0xDB26
        Source address:       192.168.10.0
        Destination address:  192.168.20.0
        ☐ IP Options:         [...]
      IP Payload
```

96 bytes. (L3: 74 bytes.) Use 'Field modifier' to generate flows/streams.

Figure 15-45 *Stream Group Configuration-3*



N2X Packets and Protocols: Session 15 (Administrator) on AGILENT-DEM

000:00:06

Start Traffic and Measurements on All Ports

Setup - Traffic

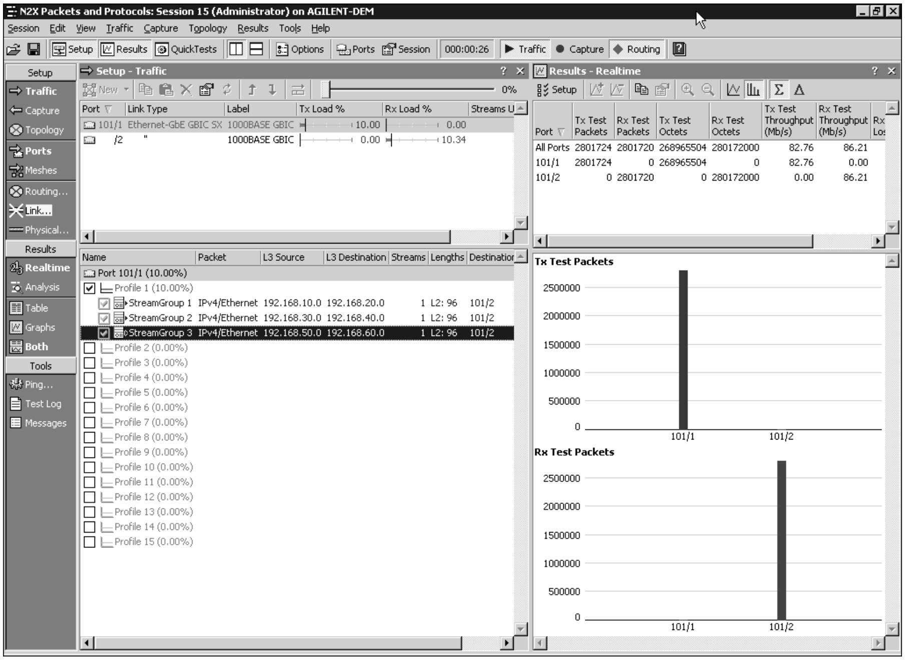
Port	Link Type	Label	Tx Load %	Rx Load %
101/1	Ethernet-GbE GBIC SX	1000BASE GBIC	10.00	0.00
/2	"	1000BASE GBIC	0.00	10.00

Name	Packet	L3 Source	L3 Destination	Streams	Lengths	Destination
Port 101/1 (10.00%)						
☑ Profile 1 (10.00%)						
☑ StreamGroup 1	IPv4/Ethernet	192.168.10.0	192.168.20.0	1	L2: 96	101/2
☑ StreamGroup 2	IPv4/Ethernet	192.168.30.0	192.168.40.0	1	L2: 96	101/2
☑ StreamGroup 3	IPv4/Ethernet	192.168.50.0	192.168.60.0	1	L2: 96	101/2
☐ Profile 2 (0.00%)						
☐ Profile 3 (0.00%)						
☐ Profile 4 (0.00%)						
☐ Profile 5 (0.00%)						
☐ Profile 6 (0.00%)						
☐ Profile 7 (0.00%)						
☐ Profile 8 (0.00%)						
☐ Profile 9 (0.00%)						
☐ Profile 10 (0.00%)						
☐ Profile 11 (0.00%)						
☐ Profile 12 (0.00%)						
☐ Profile 13 (0.00%)						
☐ Profile 14 (0.00%)						
☐ Profile 15 (0.00%)						

Port	Tx Test Packets	Rx Test Packets	Tx Test Octets	Rx Test Octets	Tx Test Throughput (Mb/s)	Rx Test Throughput (Mb/s)	Rx Packet Loss
All Ports							n/a
101/1							n/a
101/2							n/a

Step 5 After the traffic has started, the counters indicate the real time results, as shown in Figure 15-46.

Figure 15-46 *Traffic Test*



Port	Link Type	Label	Tx Load %	Rx Load %	Streams U
101/1	Ethernet-GbE GBIC SX	1000BASE GBIC	10.00	0.00	
/2	"	1000BASE GBIC	0.00	10.34	

Port	Tx Test Packets	Rx Test Packets	Tx Test Octets	Rx Test Octets	Tx Test Throughput (Mb/s)	Rx Test Throughput (Mb/s)	Rx Los
All Ports	2801724	2801720	268965504	280172000	82.76	86.21	
101/1	2801724	0	268965504	0	82.76	0.00	
101/2	0	2801720	0	280172000	0.00	86.21	

Name	Packet	L3 Source	L3 Destination	Streams	Lengths	Destinatior
Port 101/1 (10.00%)						
☑ Profile 1 (10.00%)						
☑ StreamGroup 1	IPv4/Ethernet	192.168.10.0	192.168.20.0	1	L2: 96	101/2
☑ StreamGroup 2	IPv4/Ethernet	192.168.30.0	192.168.40.0	1	L2: 96	101/2
☑ StreamGroup 3	IPv4/Ethernet	192.168.50.0	192.168.60.0	1	L2: 96	101/2
☐ Profile 2 (0.00%)						
☐ Profile 3 (0.00%)						
☐ Profile 4 (0.00%)						
☐ Profile 5 (0.00%)						
☐ Profile 6 (0.00%)						
☐ Profile 7 (0.00%)						
☐ Profile 8 (0.00%)						
☐ Profile 9 (0.00%)						
☐ Profile 10 (0.00%)						
☐ Profile 11 (0.00%)						
☐ Profile 12 (0.00%)						
☐ Profile 13 (0.00%)						
☐ Profile 14 (0.00%)						
☐ Profile 15 (0.00%)						

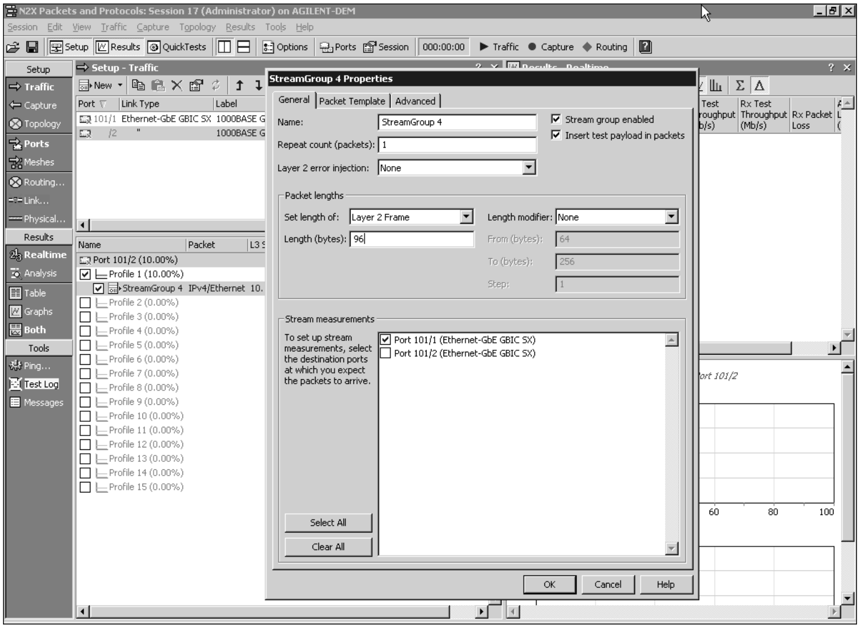
Step 6 The next step is to configure MPLS VPN traffic originated from the emulated PE router prefixes to the emulated local CE router prefixes via the DUT.

Step 7 Highlight **Port 101/2** in the Setup-Traffic pane and, in the Traffic Profiles pane, right-click the first profile and select **New Stream Group**.

Step 8 Step 7 creates a new stream group under the selected profile. Double-click the stream group to open the properties for the stream group. Under the General tab in the StreamGroup 4 Properties window, change the properties as shown in Figure 15-47. Also, make sure Port 101/1 is identified as a valid traffic destination.

Step 9 Under the Packet Template tab, right-click the **Ethernet Payload** section and select **New**, as illustrated in Figure 15-48.

Figure 15-47 *PE Stream Group Configuration-1*



N2X Packets and Protocols: Session 17 (Administrator) on AGILENT-DEM

StreamGroup 4 Properties

Name: StreamGroup 4

Repeat count (packets): 1

Layer 2 error injection: None

☑ Stream group enabled

☑ Insert test payload in packets

Packet lengths

Set length of: Layer 2 Frame

Length modifier: None

Length (bytes): 96

From (bytes): 64

To (bytes): 256

Step: 1

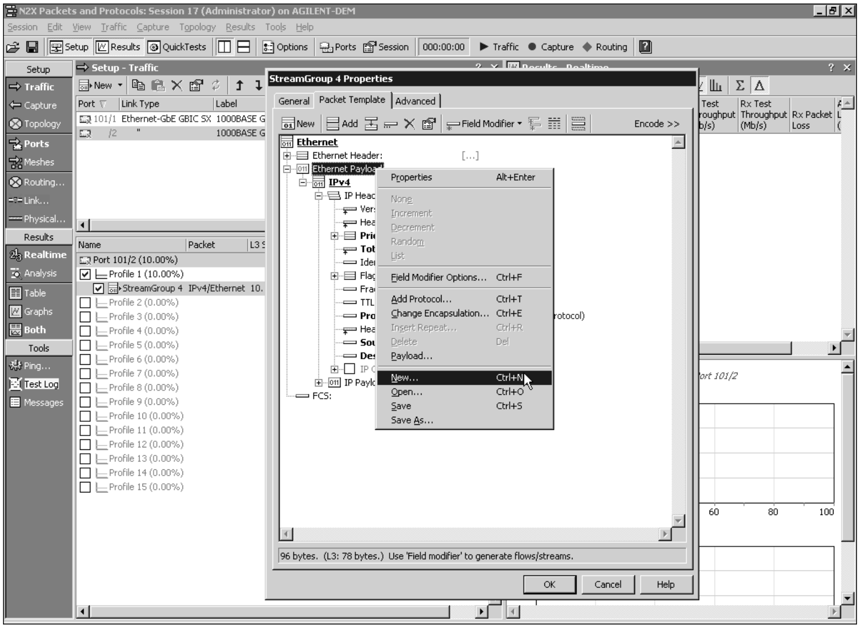
Stream measurements

To set up stream measurements, select the destination ports at which you expect the packets to arrive.

☑ Port 101/1 (Ethernet-GbE GBIC SX)

☐ Port 101/2 (Ethernet-GbE GBIC SX)

Figure 15-48 *PE Stream Group Configuration-2*



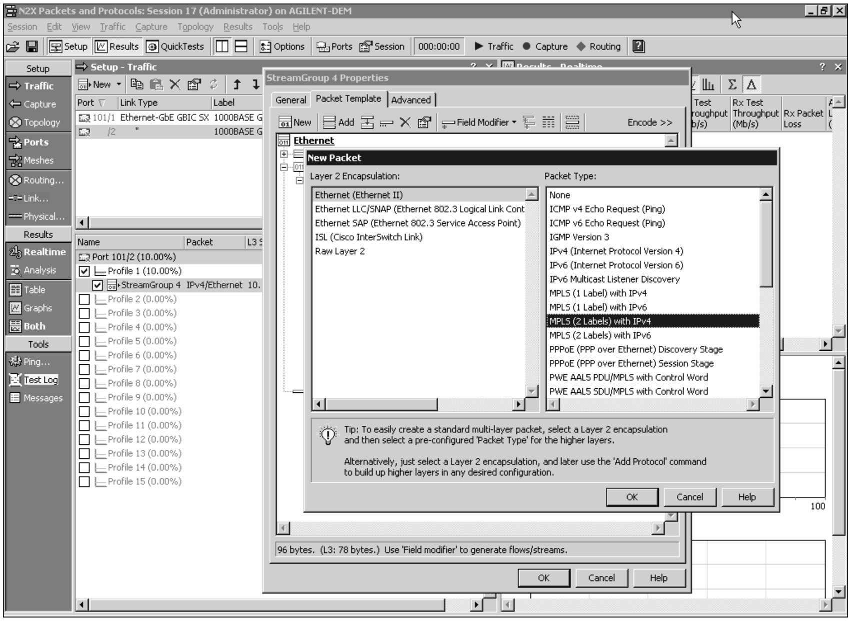
N2X Packets and Protocols: Session 17 (Administrator) on AGILENT-DEM

StreamGroup 4 Properties

96 bytes. (L3: 78 bytes.) Use 'Field modifier' to generate flows/streams.

Step 10 This opens the New Packet window, as shown in Figure 15-49. In the New Packet window, select **MPLS (2 Labels) with IPv4** because you are emulating a VPN route that will require two labels—a VPN label and a transport label. Click **OK** to close the New Packet window.

Figure 15-49 *PE Stream Group Configuration-3*


N2X Packets and Protocols: Session 17 (Administrator) on AGILENT-DEM
Session Edit View Traffic Capture Topology Results Tools Help
Setup Results QuickTests Options Ports Session 000:00:00 Traffic Capture Routing
Setup Traffic Capture Topology Ports Meshes Routing... Link... Physical...
Results Realtime Analysis Table Graphs Both
Tools Ping... Test Log Messages
Setup - Traffic
Port Link Type Label
101/1 Ethernet-GbE GBIC SX 1000BASE G
/2 " 1000BASE G
Name Packet
Port 101/2 (10.00%)
Profile 1 (10.00%)
StreamGroup 4 IPv4/Ethernet 10.
Profile 2 (0.00%)
Profile 3 (0.00%)
Profile 4 (0.00%)
Profile 5 (0.00%)
Profile 6 (0.00%)
Profile 7 (0.00%)
Profile 8 (0.00%)
Profile 9 (0.00%)
Profile 10 (0.00%)
Profile 11 (0.00%)
Profile 12 (0.00%)
Profile 13 (0.00%)
Profile 14 (0.00%)
Profile 15 (0.00%)
StreamGroup 4 Properties
General Packet Template Advanced
New Add Field Modifier Encode >>
Ethernet
New Packet
Layer 2 Encapsulation:
Ethernet (Ethernet II)
Ethernet LLC/SNAP (Ethernet 802.3 Logical Link Cont
Ethernet SAP (Ethernet 802.3 Service Access Point)
ISL (Cisco InterSwitch Link)
Raw Layer 2
Packet Type:
None
ICMP v4 Echo Request (Ping)
ICMP v6 Echo Request (Ping)
IGMP Version 3
IPv4 (Internet Protocol Version 4)
IPv6 (Internet Protocol Version 6)
IPv6 Multicast Listener Discovery
MPLS (1 Label) with IPv4
MPLS (1 Label) with IPv6
MPLS (2 Labels) with IPv4
MPLS (2 Labels) with IPv6
PPPoE (PPP over Ethernet) Discovery Stage
PPPoE (PPP over Ethernet) Session Stage
PWE AAL5 PDU/MPLS with Control Word
PWE AAL5 SDU/MPLS with Control Word
OK Cancel Help
Results - Realtime
Test Throughput (Mb/s) Rx Test Throughput (Mb/s) Rx Packet Loss
100
OK Cancel Help

Tip: To easily create a standard multi-layer packet, select a Layer 2 encapsulation and then select a pre-configured 'Packet Type' for the higher layers.

Alternatively, just select a Layer 2 encapsulation, and later use the 'Add Protocol' command to build up higher layers in any desired configuration.

96 bytes. (L3: 78 bytes.) Use 'Field modifier' to generate flows/streams.

Step 11 Prior to adding the appropriate label values, verify the label values from the DUT for all three VPN prefixes that will function as destinations for the three VPN streams to be created, as shown in Example 15-6.

Example 15-6 *Label Values on DUT*

```
DUT#show mpls forwarding vrf vpn1 192.168.10.0 detail
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
16     Untagged    192.168.10.0/24[V]   \
                                     0          Gi0/1.1    172.16.1.1
        MAC/Encaps=0/0, MRU=1504, Tag Stack{}
        VPN route: vpn1
        No output feature configured
DUT#show mpls forwarding vrf vpn2 192.168.30.0 detail
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
28     Untagged    192.168.30.0/24[V]   \
                                     0          Gi0/1.2    172.16.2.1
        MAC/Encaps=0/0, MRU=1504, Tag Stack{}
        VPN route: vpn2
        No output feature configured
```

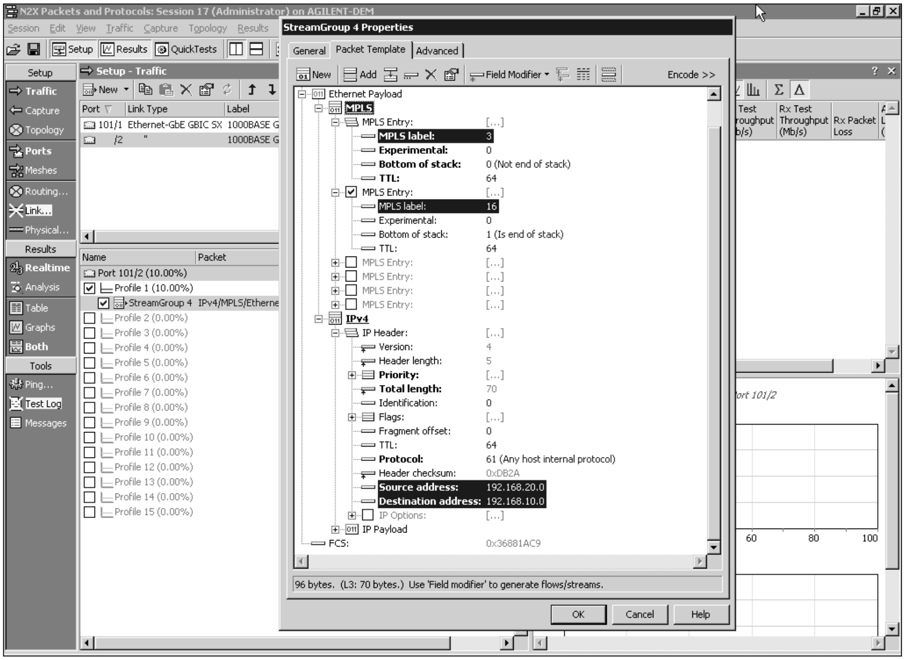
continues

Example 15-6 *Label Values on DUT (Continued)*

```
DUT#show mpls forwarding vrf vpn3 192.168.50.0 detail
Local  Outgoing    Prefix             Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id       switched   interface
26     Untagged    192.168.50.0/24[V]   \
                                      0          Gi0/1.3    172.16.3.1
        MAC/Encaps=0/0, MRU=1504, Tag Stack{}
        VPN route: vpn3
        No output feature configured
```

Step 12 Under the Packet Template tab, expand the MPLS headers as well as the IP headers, and enter the appropriate values for the top and bottom labels as well as the source and destination addresses, as shown in Figure 15-50. Click **OK** to close this window.

Figure 15-50 *PE Stream Group Configuration-4*

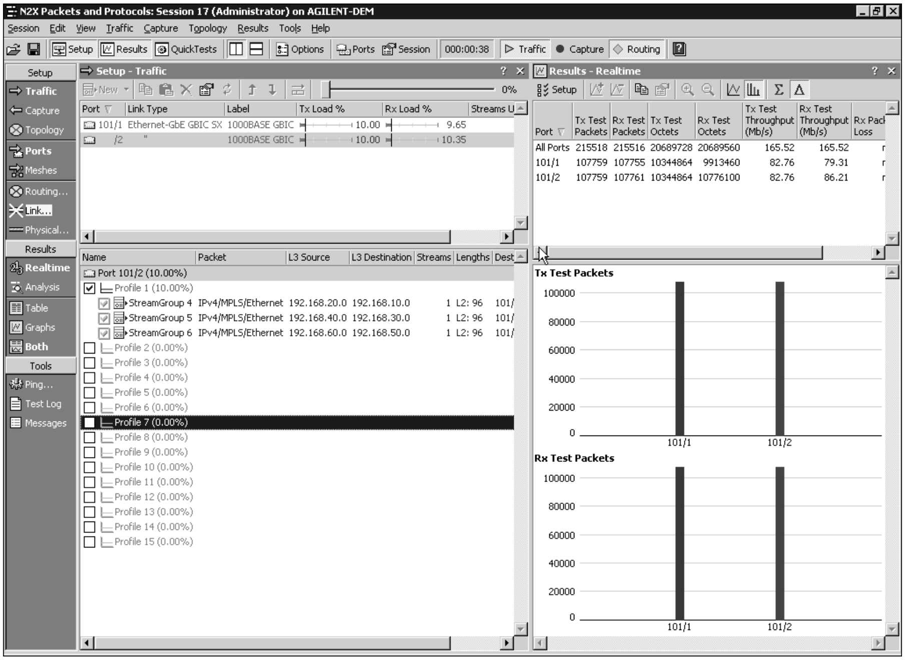


```
Ethernet Payload
  MPLS
    MPLS Entry:            [...]
      MPLS label:          3
      Experimental:        0
      Bottom of stack:     0 (Not end of stack)
      TTL:                 64
    ☑ MPLS Entry:          [...]
      MPLS label:          16
      Experimental:        0
      Bottom of stack:     1 (Is end of stack)
      TTL:                 64
    ☐ MPLS Entry:          [...]
    ☐ MPLS Entry:          [...]
    ☐ MPLS Entry:          [...]
    ☐ MPLS Entry:          [...]
  IPv4
    IP Header:             [...]
      Version:             4
      Header length:       5
      Priority:            [...]
      Total length:        70
      Identification:      0
      Flags:               [...]
      Fragment offset:     0
      TTL:                 64
      Protocol:            61 (Any host internal protocol)
      Header checksum:     0xDB2A
      Source address:      192.168.20.0
      Destination address: 192.168.10.0
      ☐ IP Options:        [...]
    IP Payload
FCS:                       0x36881AC9
96 bytes. (L3: 70 bytes.) Use 'Field modifier' to generate flows/streams.
```

Step 13 Repeat Steps 7 through 12 to add two more streams for prefixes mapping to VPNs VPN2 and VPN3.

Step 14 Finally, click the **Traffic** button in the toolbar to start the traffic. Once the traffic has started, the counters will indicate the results in real time, as shown in Figure 15-51.

Figure 15-51 *PE Traffic Test—Bidirectional*



Port	Link Type	Label	Tx Load %	Rx Load %	Streams U
101/1	Ethernet-GbE GBIC SX	1000BASE GBIC	10.00	9.65	
/2	"	1000BASE GBIC	10.00	10.35	

Name	Packet	L3 Source	L3 Destination	Streams	Lengths	Dest
Port 101/2 (10.00%)						
☑ Profile 1 (10.00%)						
☑ StreamGroup 4	IPv4/MPLS/Ethernet	192.168.20.0	192.168.10.0	1	L2: 96	101/
☑ StreamGroup 5	IPv4/MPLS/Ethernet	192.168.40.0	192.168.30.0	1	L2: 96	101/
☑ StreamGroup 6	IPv4/MPLS/Ethernet	192.168.60.0	192.168.50.0	1	L2: 96	101/
☐ Profile 2 (0.00%)						
☐ Profile 3 (0.00%)						
☐ Profile 4 (0.00%)						
☐ Profile 5 (0.00%)						
☐ Profile 6 (0.00%)						
☐ Profile 7 (0.00%)						
☐ Profile 8 (0.00%)						
☐ Profile 9 (0.00%)						
☐ Profile 10 (0.00%)						
☐ Profile 11 (0.00%)						
☐ Profile 12 (0.00%)						
☐ Profile 13 (0.00%)						
☐ Profile 14 (0.00%)						
☐ Profile 15 (0.00%)						

Port	Tx Test Packets	Rx Test Packets	Tx Test Octets	Rx Test Octets	Tx Test Throughput (Mb/s)	Rx Test Throughput (Mb/s)	Rx Pack Loss
All Ports	215518	215516	20689728	20689560	165.52	165.52	r
101/1	107759	107755	10344864	9913460	82.76	79.31	r
101/2	107759	107761	10344864	10776100	82.76	86.21	r

Testing L2 VPN with Agilent N2X

This section provides the steps to test a DUT for L2 VPN functionality in conjunction with the Agilent N2X.

Topology for L2 VPN Testing

The topology used in the test setup attempts to emulate the network as shown in Figure 15-52. A single Cisco router is configured to perform the functions of Router PE1 in all test cases for L2 VPN. All other associated CE routers and core routers shown in Figure 15-52 are emulated using two test ports on each of the route/traffic generators.

All directly connected CE routers to PE1 in the topology shown in Figure 15-52 are emulated using logical links (sub-interfaces) with a single physical interface connecting to the route/traffic generator. A second link connecting to the PE from the route/traffic generators emulates the MPLS domain (consisting of Routers P1, PE2, PE3, and PE4) with the appropriate emulated PE routers advertising VC prefixes mapping to the networks to be advertised by Routers CE2, CE4, and CE6. In all route/traffic generators, no emulation of the remote PE-CE Routing protocol is performed. The physical connectivity to emulate the network shown in Figure 15-52 is illustrated in Figure 15-53.

Figure 15-52 *Topology for L2 VPN Testing*

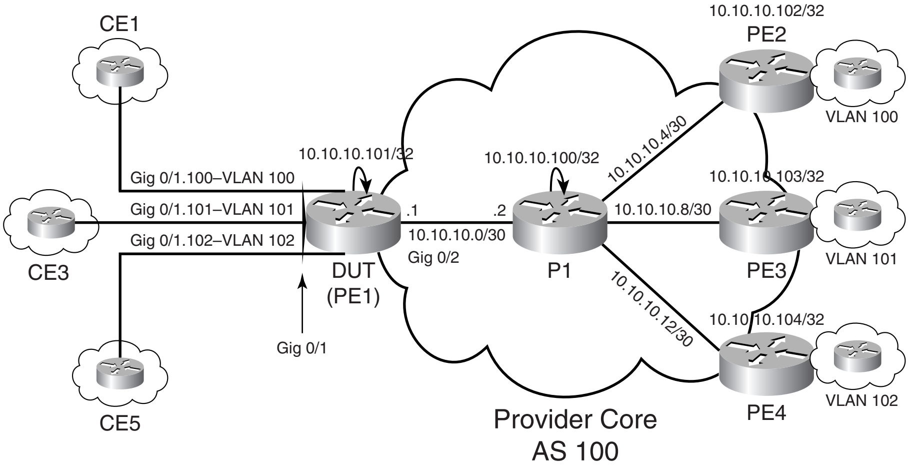
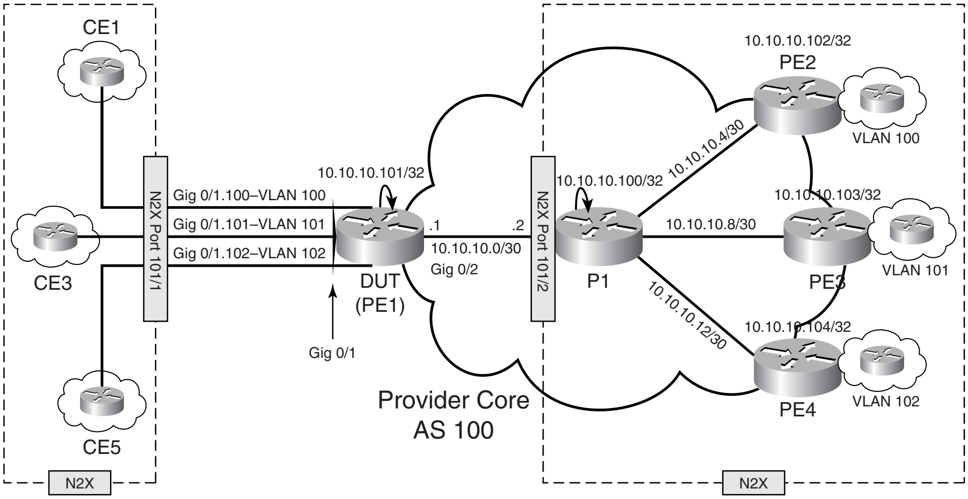


Figure 15-53 *Physical Connectivity*



Testing L2 MPLS VPN (AToM) Functionality

To test MPLS VPN PE functionality, a network is emulated, as shown in Figure 15-53, in which the DUT is PE1. The traffic generator and its ports are used to configure and emulate the rest of the network shown in Figure 15-53.

Conditions and Prerequisites

The following outlines the conditions and prerequisites for the implementation of the test topology shown in Figure 15-52:

- This test requires two ports on the route/traffic generator; one port to emulate CE connectivity to the DUT and the other port to emulate the MPLS domain, which includes provider core routers and PE routers and remote CE routers belonging to multiple VPNs.
- The test involves the emulation of three CE routers belonging to different L2 VPNs on three different VLANs—100, 101, and 102—connecting to the DUT using Gigabit Ethernet sub-interfaces.

Example 15-7 shows the configuration of the DUT used for testing MPLS VPN functionality.

Example 15-7 *DUT Configuration for L2 VPN Test*

```
hostname DUT
!
ip cef
!
interface Loopback0
 ip address 10.10.10.101 255.255.255.255
 no ip directed-broadcast
!
interface GigabitEthernet0/1
 description Connected to traffic generator port 1(emulate local CE connections)
 no ip address
 no ip directed-broadcast
!
interface GigabitEthernet0/1.100
 encapsulation dot1Q 100
 no cdp enable
 xconnect 10.10.10.102 100 encapsulation mpls
!
interface GigabitEthernet0/1.101
 encapsulation dot1Q 101
 no cdp enable
 xconnect 10.10.10.103 101 encapsulation mpls
!
interface GigabitEthernet0/1.102
 encapsulation dot1Q 102
 no cdp enable
 xconnect 10.10.10.104 102 encapsulation mpls
!
interface GigabitEthernet0/2
 ip address 10.10.10.1 255.255.255.252
 mpls label protocol ldp
 tag-switching ip
!
router ospf 100
 log-adjacency-changes
 network 10.10.10.0 0.0.0.3 area 0
 network 10.10.10.101 0.0.0.0 area 0
```

Testing L2 VPN Functionality with Agilent N2X

For this test, use the Agilent N2X chassis along with a two-port GE line card to test L2 VPN PE functionality of the DUT. All configurations for route as well as traffic generation are performed on the N2X Packets 6.4 System Release. The version used for all screenshots in this chapter is 6.4. Prior to all the configurations in this chapter, the Agilent software has to be installed on a controller system that can be then used to configure the N2X chassis and cards. This will involve purchasing the appropriate licenses and software followed by installation. The installation procedures can be found online at http://www.agilent.com. After installation, verify that the IP address assigned to the N2X chassis is reachable from the controller system prior to configuration.

Prior to L2 VPN configuration on the N2X, remote connectivity to the N2X chassis needs to be established. This is explained in the L3 VPN N2X Packets and Protocols Initial Configuration section. Upon completion, the following steps are implemented on the N2X chassis for the configuration and implementation of L2 VPN. It is assumed that prior to the following configuration, the IP addressing and MAC addressing has been performed on the appropriate ports to the requirements outlined in Figure 15-53. It is important to implement the configuration of sub-interfaces on the CE emulation port with VLAN enabled (VLAN 100, 101, and 102) and the core emulation port will need to have OSPF and LDP enabled (OSPF for IGP and LDP for label exchange and MPLS operation).

Configuring OSPF as the IGP for L2 VPN

The configuration of OSPF as the IGP for implementation and verification of L2 VPN functionality is similar to the emulation of the network when implementing L3 VPN. The configuration consists of defining adjacency between the DUT and the router 10.10.10.2 (P1) where the router 10.10.10.2 with router ID 10.10.10.100 generates LSAs that identify the topology of the core network as advertised by OSPF to the DUT. The configuration is the same as shown earlier in the N2X OSPF PE-CE and OSPF IGP Configuration section under Layer 3 VPN testing with N2X.

Once the configuration is performed as shown, enable the OSPF sessions in the core as depicted in the "N2X OSPF PE-CE and OSPF IGP Configuration" section. Once the neighbor relationship is complete, the DUT will see routes as generated by the core port, as illustrated in Example 15-8.

Example 15-8 *OSPF Verification Core*

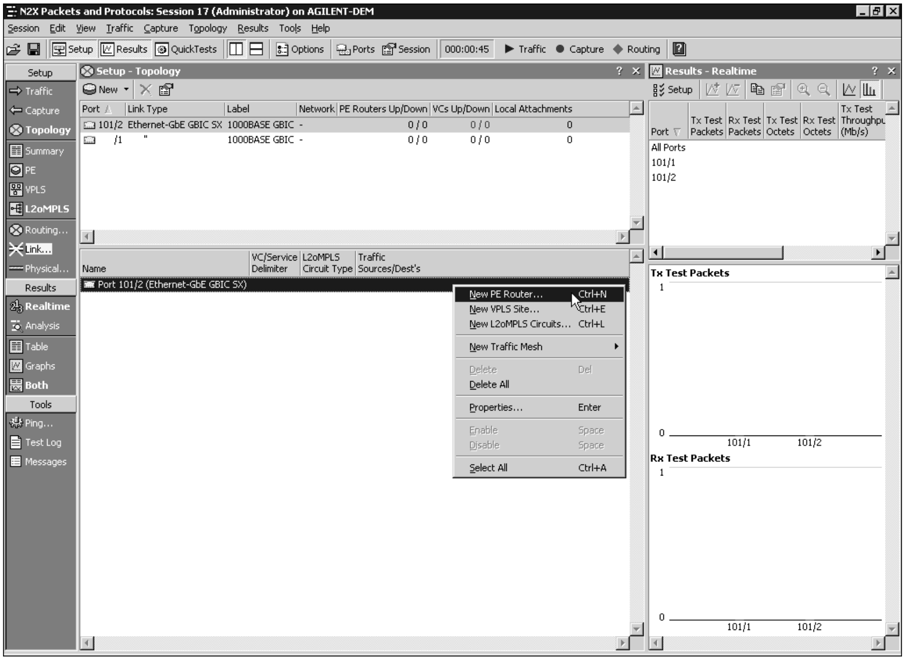
```
DUT#show ip route ospf
     10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
        10.10.10.8/30 [110/2] via 10.10.10.2, 00:00:11, GigabitEthernet0/2
        10.10.10.12/30 [110/2] via 10.10.10.2, 00:00:11, GigabitEthernet0/2
        10.10.10.4/30 [110/2] via 10.10.10.2, 00:00:11, GigabitEthernet0/2
        10.10.10.104/32 [110/3] via 10.10.10.2, 00:00:11, GigabitEthernet0/2
        10.10.10.102/32 [110/3] via 10.10.10.2, 00:00:11, GigabitEthernet0/2
        10.10.10.103/32 [110/3] via 10.10.10.2, 00:00:11, GigabitEthernet0/2
        10.10.10.100/32 [110/2] via 10.10.10.2, 00:00:11, GigabitEthernet0/2
```

Configuring PE Routers and LDP for L2 VPN

The following steps outline the configuration of remote PE router LDP sessions for the emulated SP core (PE2, PE3, and PE4):

Step 1 To configure PE routers, click the **Topology** button in the Setup bar. Select **Port 101/2** in the Setup-Topology window. Right-click the port and select the option to add a new PE router, as shown in Figure 15-54.

Figure 15-54 *Adding New PE Router-1*



Port	Link Type	Label	Network	PE Routers Up/Down	VCs Up/Down	Local Attachments
101/2	Ethernet-GbE GBIC SX	1000BASE GBIC	-	0 / 0	0 / 0	0
/1	"	1000BASE GBIC	-	0 / 0	0 / 0	0

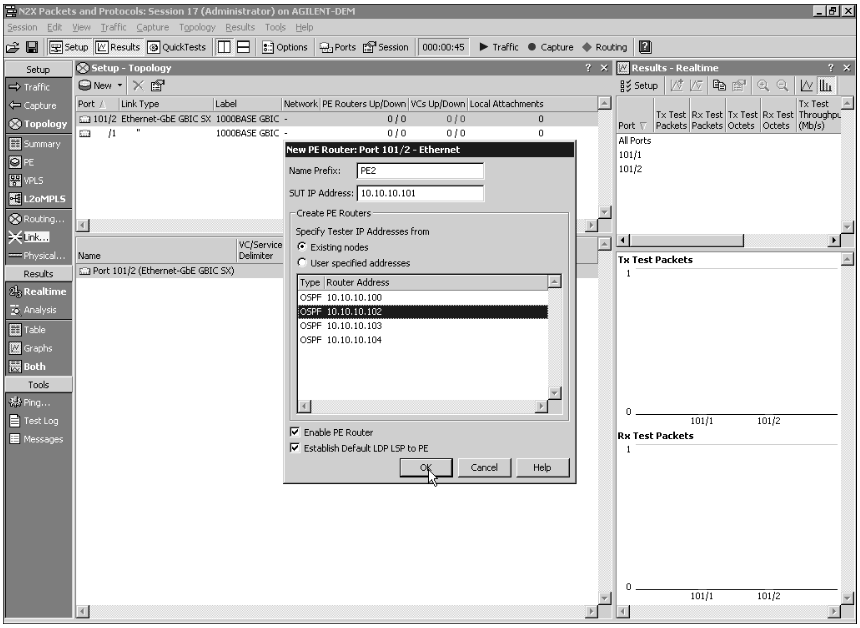
Name	VC/Service Delimiter	L2oMPLS Circuit Type	Traffic Sources/Dest's
Port 101/2 (Ethernet-GbE GBIC SX)			

Port	Tx Test Packets	Rx Test Packets	Tx Test Octets	Rx Test Octets	Tx Test Throughpu (Mb/s)
All Ports					
101/1					
101/2					

Step 2 This opens the New PE Router window shown in Figure 15-55. Configure the PE name, the SUT IP address to be 10.10.10.101 (PE1 loopback), select the PE2 loopback from the window, and click **OK**. This step also automatically creates a targeted LDP session between the two peers.

Step 3 Repeat Steps 1 and 2 to add the PE Routers PE3 and PE4 to the list of PE routers on 101/2, as shown in Figure 15-56.

Figure 15-55 *Adding New PE Router-2*



N2X Packets and Protocols: Session 17 (Administrator) on AGILENT-DEM
Session Edit View Traffic Capture Topology Results Tools Help
Setup Results QuickTests Options Ports Session 000:00:45 Traffic Capture Routing
Setup Traffic Capture Topology Summary PE VPLS L2oMPLS Routing... Link... Physical...
Results Realtime Analysis Table Graphs Both
Tools Ping... Test Log Messages
Setup - Topology
New
Results - Realtime
Setup

Port	Link Type	Label	Network	PE Routers Up/Down	VCs Up/Down	Local Attachments
101/2	Ethernet-GbE GBIC SX	1000BASE GBIC	-	0 / 0	0 / 0	0
/1	"	1000BASE GBIC	-	0 / 0	0 / 0	0

Name	VC/Service Delimiter
Port 101/2 (Ethernet-GbE GBIC SX)	

New PE Router: Port 101/2 - Ethernet

Name Prefix: PE2

SUT IP Address: 10.10.10.101

Create PE Routers

Specify Tester IP Addresses from

● Existing nodes

○ User specified addresses

Type	Router Address
OSPF	10.10.10.100
OSPF	10.10.10.102
OSPF	10.10.10.103
OSPF	10.10.10.104

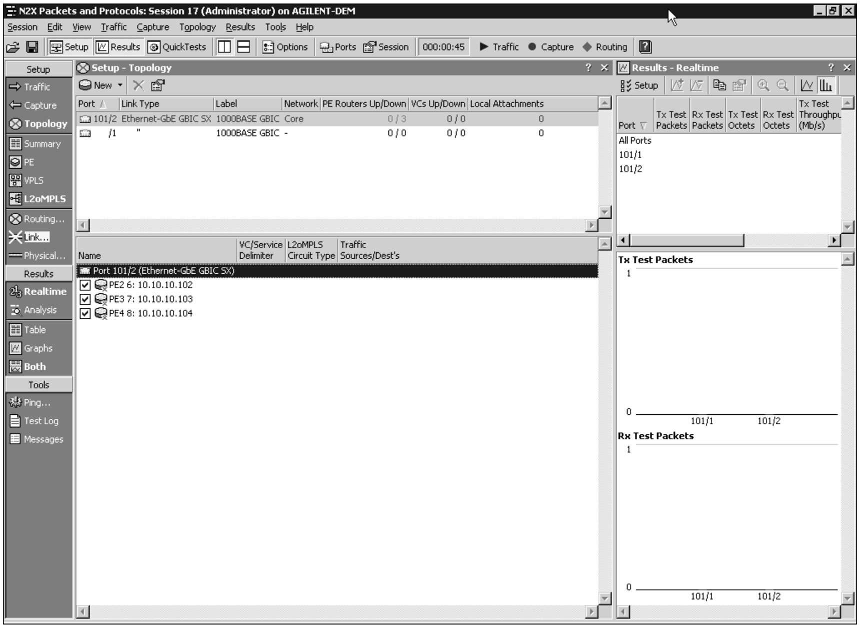
☑ Enable PE Router

☑ Establish Default LDP LSP to PE

OK Cancel Help

Port	Tx Test Packets	Rx Test Packets	Tx Test Octets	Rx Test Octets	Tx Test Throughput (Mb/s)
All Ports					
101/1					
101/2					

Figure 15-56 *Adding New PE Router-3*



N2X Packets and Protocols: Session 17 (Administrator) on AGILENT-DEM
Session Edit View Traffic Capture Topology Results Tools Help
Setup Results QuickTests Options Ports Session 000:00:45 Traffic Capture Routing
Setup Traffic Capture Topology Summary PE VPLS L2oMPLS Routing... Link... Physical...
Results Realtime Analysis Table Graphs Both
Tools Ping... Test Log Messages
Setup - Topology
New
Results - Realtime
Setup

Port	Link Type	Label	Network	PE Routers Up/Down	VCs Up/Down	Local Attachments
101/2	Ethernet-GbE GBIC SX	1000BASE GBIC	Core	0 / 3	0 / 0	0
/1	"	1000BASE GBIC	-	0 / 0	0 / 0	0

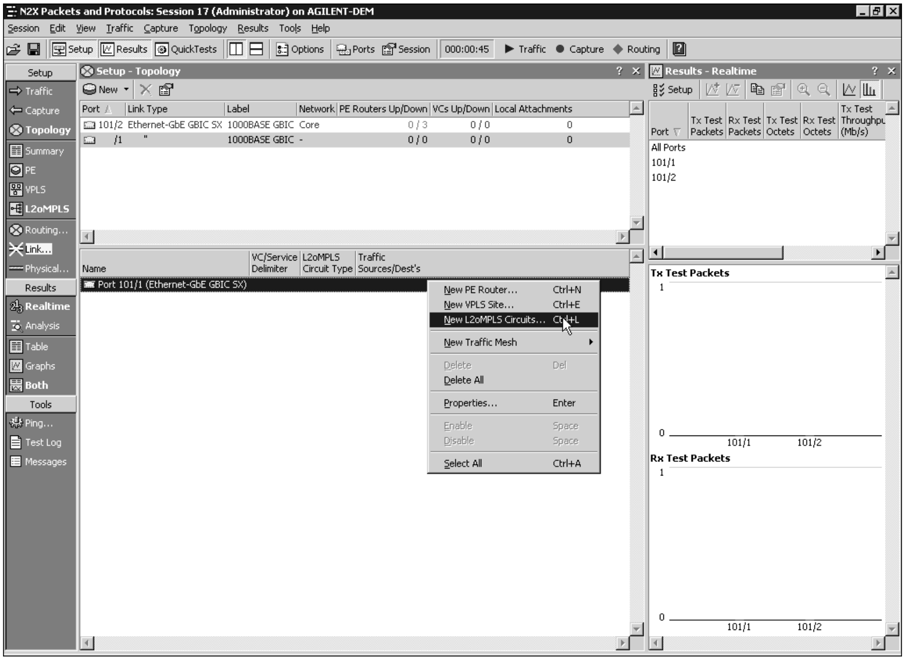
Name	VC/Service Delimiter	L2oMPLS Circuit Type	Traffic Sources/Dest's
Port 101/2 (Ethernet-GbE GBIC SX)			
☑ PE2 6: 10.10.10.102			
☑ PE3 7: 10.10.10.103			
☑ PE4 8: 10.10.10.104			

Port	Tx Test Packets	Rx Test Packets	Tx Test Octets	Rx Test Octets	Tx Test Throughput (Mb/s)
All Ports					
101/1					
101/2					

Step 4 The next step is to add L2 over MPLS tunnels on Port 101/1, which is the port functioning as the access port.

To add an L2 over MPLS tunnel, select the access Port 101/1, and, in the Setup-Topology window, right-click the same and select the option to add a new L2oMPLS circuit, as shown, in Figure 15-57.

Figure 15-57 *Adding New L2oMPLS Circuit-1*



Port	Link Type	Label	Network	PE Routers Up/Down	VCs Up/Down	Local Attachments
101/2	Ethernet-GbE GBIC SX	1000BASE GBIC	Core	0 / 3	0 / 0	0
/1	"	1000BASE GBIC	-	0 / 0	0 / 0	0

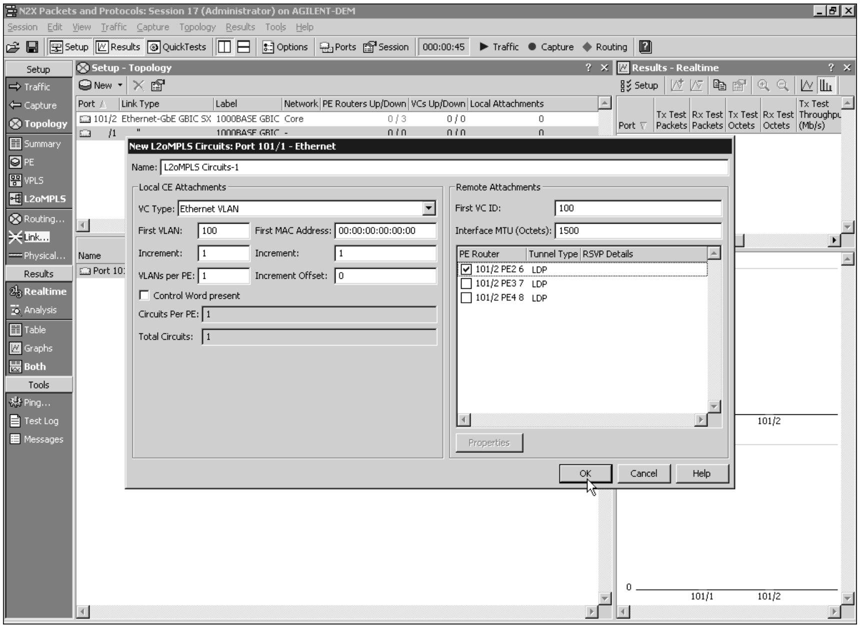
Name	VC/Service Delimiter	L2oMPLS Circuit Type	Traffic Sources/Dest's
Port 101/1 (Ethernet-GbE GBIC SX)			

Port	Tx Test Packets	Rx Test Packets	Tx Test Octets	Rx Test Octets	Tx Test Throughpu (Mb/s)
All Ports					
101/1					
101/2					

Step 5 In the L2oMPLS Circuits window, select the VC Type to be **Ethernet VLAN**. Enter **100** for the VLAN ID and **100** for the VC ID, select the endpoint of the tunnel to be the PE2 PE router, and click **OK**, as shown in Figure 15-58.

Step 6 Repeat Steps 4 and 5 for the two other L2oMPLS circuits mapping to VLAN 101 terminating on PE3, and VLAN 102 terminating on PE4 to create three total L2oMPLS circuits, as shown in Figure 15-59.

Figure 15-58 *Adding New L2oMPLS Circuit-2*


N2X Packets and Protocols: Session 17 (Administrator) on AGILENT-DEM
Session Edit View Traffic Capture Topology Results Tools Help
Setup Results QuickTests Options Ports Session 000:00:45 Traffic Capture Routing
Setup Traffic Capture Topology Summary PE VPLS L2oMPLS Routing... Link... Physical...
Results Realtime Analysis Table Graphs Both
Tools Ping... Test Log Messages
Setup - Topology
New
Results - Realtime
Setup
Port Tx Test Packets Rx Test Packets Tx Test Octets Rx Test Octets Tx Test Throughpu (Mb/s)
101/2
0 101/1 101/2
Name
Port 10
Properties
OK Cancel Help

Port	Link Type	Label	Network	PE Routers Up/Down	VCs Up/Down	Local Attachments
101/2	Ethernet-GbE GBIC SX	1000BASE GBIC	Core	0 / 3	0 / 0	0
/1	"	1000BASE GBIC	-	0 / 0	0 / 0	0

New L2oMPLS Circuits: Port 101/1 - Ethernet

Name: L2oMPLS Circuits-1

Local CE Attachments

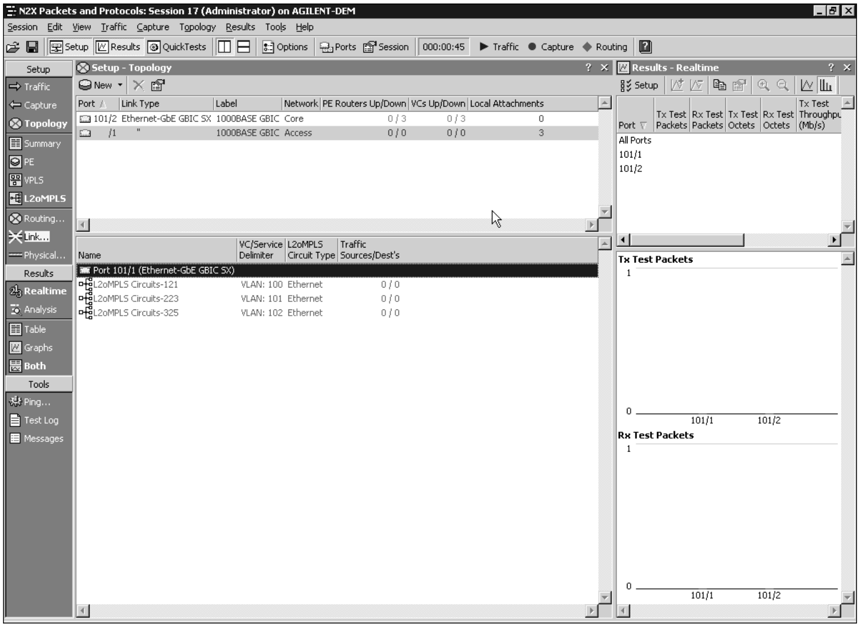
VC Type: Ethernet VLAN
First VLAN: 100
First MAC Address: 00:00:00:00:00:00
Increment: 1
Increment: 1
VLANs per PE: 1
Increment Offset: 0
☐ Control Word present
Circuits Per PE: 1
Total Circuits: 1

Remote Attachments

First VC ID: 100
Interface MTU (Octets): 1500

PE Router	Tunnel Type	RSVP Details
☑ 101/2 PE2 6	LDP	
☐ 101/2 PE3 7	LDP	
☐ 101/2 PE4 8	LDP	

Figure 15-59 *Adding New L2oMPLS Circuit-3*

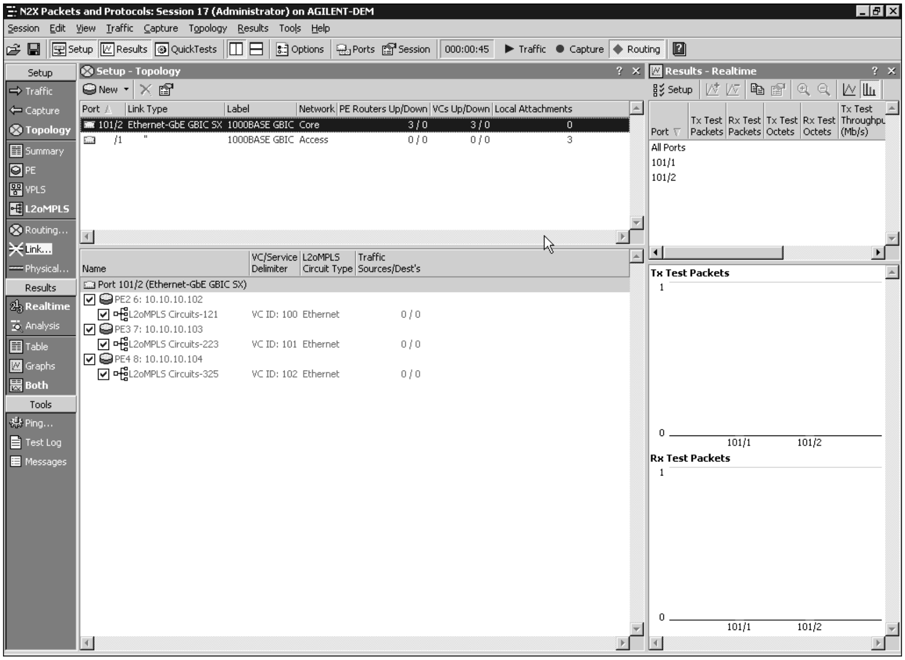

N2X Packets and Protocols: Session 17 (Administrator) on AGILENT-DEM
Session Edit View Traffic Capture Topology Results Tools Help
Setup Results QuickTests Options Ports Session 000:00:45 Traffic Capture Routing
Setup Traffic Capture Topology Summary PE VPLS L2oMPLS Routing... Link... Physical...
Results Realtime Analysis Table Graphs Both
Tools Ping... Test Log Messages
Setup - Topology
New
Results - Realtime
Setup
Port Tx Test Packets Rx Test Packets Tx Test Octets Rx Test Octets Tx Test Throughpu (Mb/s)
All Ports
101/1
101/2
Tx Test Packets
1
0 101/1 101/2
Rx Test Packets
1
0 101/1 101/2

Port	Link Type	Label	Network	PE Routers Up/Down	VCs Up/Down	Local Attachments
101/2	Ethernet-GbE GBIC SX	1000BASE GBIC	Core	0 / 3	0 / 3	0
/1	"	1000BASE GBIC	Access	0 / 0	0 / 0	3

Name	VC/Service Delimiter	L2oMPLS Circuit Type	Traffic Sources/Dest's
Port 101/1 (Ethernet-GbE GBIC SX)			
L2oMPLS Circuits-121	VLAN: 100	Ethernet	0 / 0
L2oMPLS Circuits-223	VLAN: 101	Ethernet	0 / 0
L2oMPLS Circuits-325	VLAN: 102	Ethernet	0 / 0

Step 7 Start the routing engine, and the PE routers and L2 circuits must come up, as shown in Figure 15-60.

Figure 15-60 *Verification on N2X L2oMPLS*



Port	Link Type	Label	Network	PE Routers Up/Down	VCs Up/Down	Local Attachments
101/2	Ethernet-GbE GBIC SX	1000BASE GBIC	Core	3 / 0	3 / 0	0
/1	"	1000BASE GBIC	Access	0 / 0	0 / 0	3

Name	VC/Service Delimiter	L2oMPLS Circuit Type	Traffic Sources/Dest's
Port 101/2 (Ethernet-GbE GBIC SX)			
☑ PE2 6: 10.10.10.102			
☑ L2oMPLS Circuits-121	VC ID: 100	Ethernet	0 / 0
☑ PE3 7: 10.10.10.103			
☑ L2oMPLS Circuits-223	VC ID: 101	Ethernet	0 / 0
☑ PE4 8: 10.10.10.104			
☑ L2oMPLS Circuits-325	VC ID: 102	Ethernet	0 / 0

Port	Tx Test Packets	Rx Test Packets	Tx Test Octets	Rx Test Octets	Tx Test Throughpu (Mb/s)
All Ports					
101/1					
101/2					

Step 8 Verify LDP neighbor relationship and label exchange by performing the appropriate commands on the DUT, as shown in Example 15-9.

Example 15-9 *DUT Verification LDP and L2 VPN States*

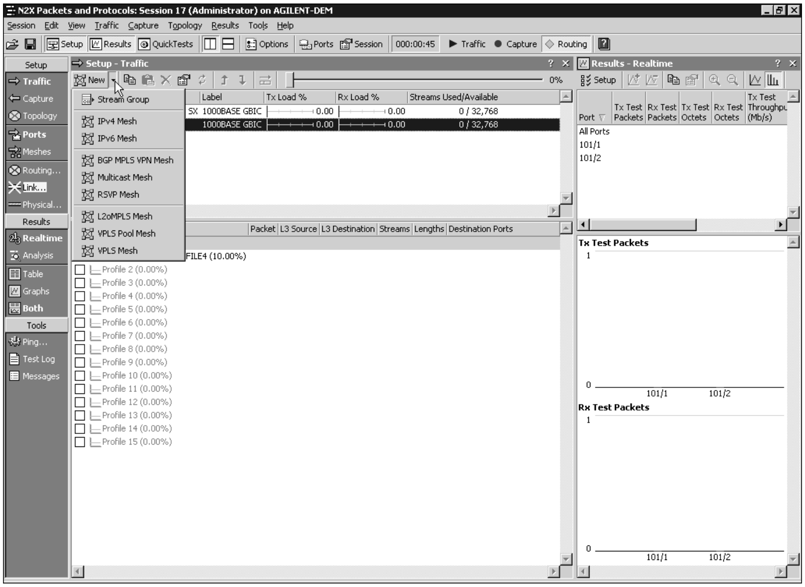
```
DUT#show mpls l2transport vc

Local intf     Local circuit          Dest address    VC ID      Status
-------------  ---------------------- --------------- ---------- ----------
Gi0/1.100      Eth VLAN 100           10.10.10.102    100        UP
Gi0/1.101      Eth VLAN 101           10.10.10.103    101        UP
Gi0/1.102      Eth VLAN 102           10.10.10.104    102        UP
```

Traffic Generation in L2 VPN

For traffic generation, you send three streams, all originating from the locally connected VLANs on the DUT, to the remote PE router loopback interfaces:

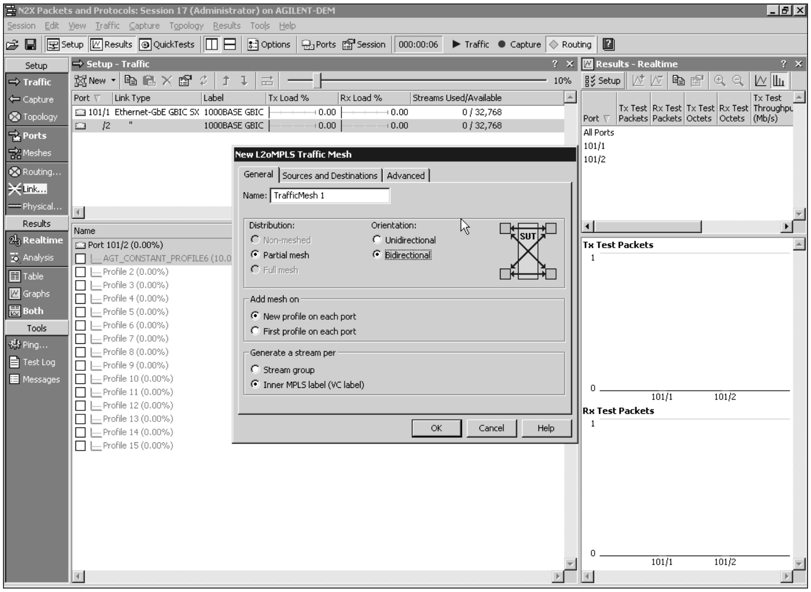
Step 1 Select the **Traffic** button in the Setup bar. In the Setup-Traffic window, click the **New** button drop-down menu and select **L2oMPLS Mesh**, as shown in Figure 15-61.

Figure 15-61 *Configuring L2oMPLS Mesh-1*



Step 2 In the New L2oMPLS Traffic Mesh window, under the General tab, select **Bidirectional** traffic, as shown in Figure 15-62.

Figure 15-62 *Configuring L2oMPLS Mesh-2*



Name: TrafficMesh 1

Distribution:
○ Non-meshed
● Partial mesh
○ Full mesh

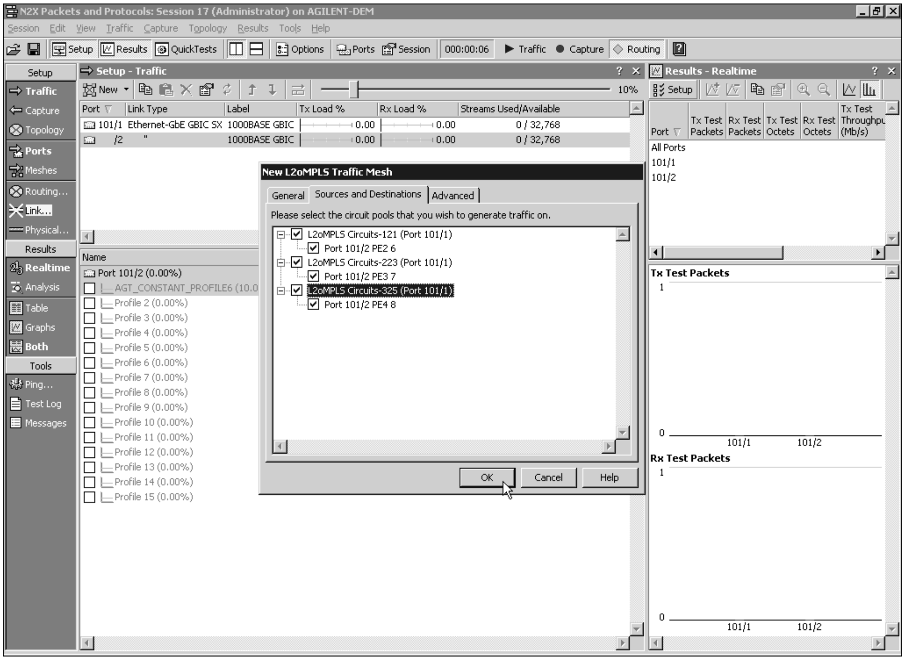
Orientation:
○ Unidirectional
● Bidirectional

Add mesh on
● New profile on each port
○ First profile on each port

Generate a stream per
○ Stream group
● Inner MPLS label (VC label)

Step 3 Under the Sources and Destinations tab, select all L2 circuits for traffic generation and click **OK**, as shown in Figure 15-63. This creates six traffic meshes.

Figure 15-63 *Configuring L2oMPLS Mesh-3*


N2X Packets and Protocols: Session 17 (Administrator) on AGILENT-DEM
Session Edit View Traffic Capture Topology Results Tools Help
Setup Results QuickTests Options Ports Session 000:00:06 Traffic Capture Routing
Setup Traffic Capture Topology Ports Meshes Routing… Link… Physical…
Results Realtime Analysis Table Graphs Both
Tools Ping… Test Log Messages
Setup - Traffic
New 10%
Results - Realtime
Setup
Tx Test Packets
Rx Test Packets
1
0
101/1
101/2
OK Cancel Help

Port	Link Type	Label	Tx Load %	Rx Load %	Streams Used/Available
101/1	Ethernet-GbE GBIC SX	1000BASE GBIC	0.00	0.00	0 / 32,768
/2	"	1000BASE GBIC	0.00	0.00	0 / 32,768

Name
Port 101/2 (0.00%)
☐ AGT_CONSTANT_PROFILE6 (10.0
☐ Profile 2 (0.00%)
☐ Profile 3 (0.00%)
☐ Profile 4 (0.00%)
☐ Profile 5 (0.00%)
☐ Profile 6 (0.00%)
☐ Profile 7 (0.00%)
☐ Profile 8 (0.00%)
☐ Profile 9 (0.00%)
☐ Profile 10 (0.00%)
☐ Profile 11 (0.00%)
☐ Profile 12 (0.00%)
☐ Profile 13 (0.00%)
☐ Profile 14 (0.00%)
☐ Profile 15 (0.00%)

Port	Tx Test Packets	Rx Test Packets	Tx Test Octets	Rx Test Octets	Tx Test Throughpu (Mb/s)
All Ports					
101/1					
101/2					

New L2oMPLS Traffic Mesh

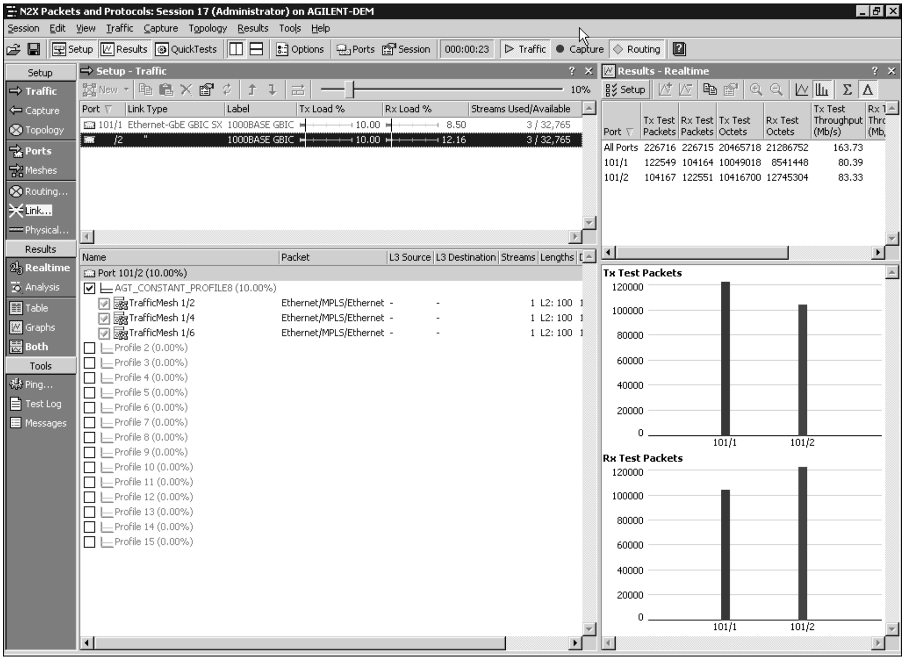
General | Sources and Destinations | Advanced

Please select the circuit pools that you wish to generate traffic on.

- ☑ L2oMPLS Circuits-121 (Port 101/1)
  - ☑ Port 101/2 PE2 6
- ☑ L2oMPLS Circuits-223 (Port 101/1)
  - ☑ Port 101/2 PE3 7
- ☑ L2oMPLS Circuits-325 (Port 101/1)
  - ☑ Port 101/2 PE4 8

Step 4 Start traffic by clicking on the **Traffic** button in the toolbar. Figure 15-64 shows the real-time results area with incremental counters on 101/1 and 101/2 depicting bidirectional traffic.

Figure 15-64 *Traffic Verification*


N2X Packets and Protocols: Session 17 (Administrator) on AGILENT-DEM
Session Edit View Traffic Capture Topology Results Tools Help
Setup Results QuickTests Options Ports Session 000:00:23 Traffic Capture Routing
Setup Traffic Capture Topology Ports Meshes Routing... Link... Physical...
Results Realtime Analysis Table Graphs Both
Tools Ping... Test Log Messages
Setup - Traffic
New
10%
Results - Realtime
Setup
Tx Test Packets
120000
100000
80000
60000
40000
20000
0
101/1
101/2
Rx Test Packets
120000
100000
80000
60000
40000
20000
0
101/1
101/2

Port	Link Type	Label	Tx Load %	Rx Load %	Streams Used/Available
101/1	Ethernet-GbE GBIC SX	1000BASE GBIC	10.00	8.50	3 / 32,765
/2	"	1000BASE GBIC	10.00	12.16	3 / 32,765

Port	Tx Test Packets	Rx Test Packets	Tx Test Octets	Rx Test Octets	Tx Test Throughput (Mb/s)
All Ports	226716	226715	20465718	21286752	163.73
101/1	122549	104164	10049018	8541448	80.39
101/2	104167	122551	10416700	12745304	83.33

Name	Packet	L3 Source	L3 Destination	Streams	Lengths
Port 101/2 (10.00%)					
☑ AGT_CONSTANT_PROFILE8 (10.00%)					
☑ TrafficMesh 1/2	Ethernet/MPLS/Ethernet	-	-	1	L2: 100
☑ TrafficMesh 1/4	Ethernet/MPLS/Ethernet	-	-	1	L2: 100
☑ TrafficMesh 1/6	Ethernet/MPLS/Ethernet	-	-	1	L2: 100
☐ Profile 2 (0.00%)					
☐ Profile 3 (0.00%)					
☐ Profile 4 (0.00%)					
☐ Profile 5 (0.00%)					
☐ Profile 6 (0.00%)					
☐ Profile 7 (0.00%)					
☐ Profile 8 (0.00%)					
☐ Profile 9 (0.00%)					
☐ Profile 10 (0.00%)					
☐ Profile 11 (0.00%)					
☐ Profile 12 (0.00%)					
☐ Profile 13 (0.00%)					
☐ Profile 14 (0.00%)					
☐ Profile 15 (0.00%)					

Step 5 Verify operation of L2oMPLS traffic on DUT, as shown in Example 15-10.

Example 15-10 *DUT Verification of L2oMPLS Traffic*

```
DUT#show mpls l2transport vc detail | inc packet
    packet totals: receive 16938670, send 20540565
    packet drops:  receive 0, seq error 0, send 0
    packet totals: receive 16938684, send 20540582
    packet drops:  receive 0, seq error 0, send 0
    packet totals: receive 16938696, send 20540596
    packet drops:  receive 0, seq error 0, send 0
```

Testing MPLS with the IXIA 1600T Platform

The section covers the following:

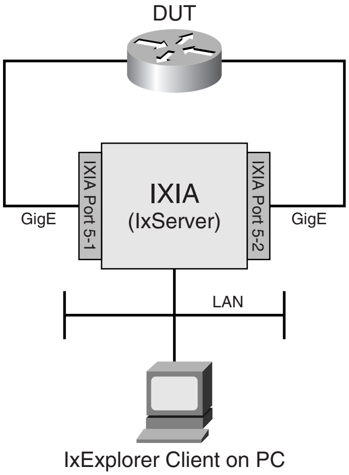
- Testing with IXIA
- Testing L3 MPLS VPN with IXIA
- PE-CE configuration on the IXIA
- Testing L2 VPN with IXIA
- Testing VPLS with IXIA

Testing with IXIA

The IXIA system is a comprehensive tool available for testing multilayer 10/100 Mbps Ethernet, Gigabit and 10 Gigabit Ethernet, ATM, and Packet over SONET switches, routers, and networks. The IXIA product family includes the chassis, load modules, the IXIA Explorer software program, and optional Tcl scripts and related software. The IXIA Explorer software provides complete configuration, control, and monitoring of all IXIA resources in the test network, and the Tcl scripts allow the user to rapidly conduct the most popular industry benchmark tests.

The user can configure and control the unit directly via back-panel connections to a keyboard, mouse, monitor, and printer. The unit can be connected to an Ethernet network, and an administrator can remotely monitor and control it using the IxExplorer software program. Multiple users can access the unit simultaneously, thereby splitting the ports within a chassis and controlling the activity and configuration of all ports and functions. Figure 15-65 shows the IXIA chassis connected to the DUT. The chassis is connected to the Ethernet LAN network.

Figure 15-65 *IXIA System and IxExplorer*



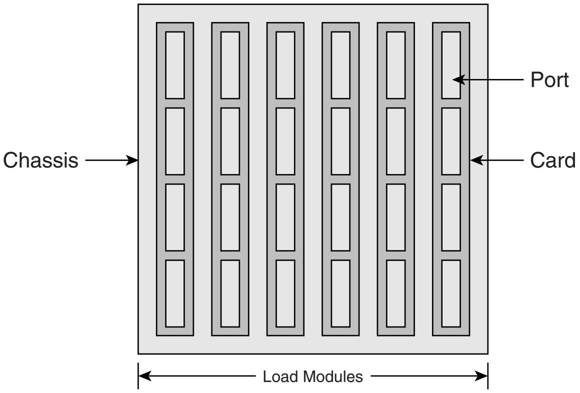
The IxExplorer software is the user's primary tool for interactive navigation, configuration, and control of the IXIA hardware. IxExplorer software that has been installed on the chassis itself can be accessed by using a monitor attached directly to the chassis. To use IxExplorer on a PC that is on the network attached to the IXIA chassis, IxExplorer software has to be installed. After initial configuration, the monitor, keyboard, and mouse need not remain attached to the chassis. If the IxExplorer is to be used from a remote system like a PC or remote workstation, the software must be installed there.

IXIA Components

The IXIA system comprises the following components, as shown in Figure 15-66:

- Chassis
- Card
- Port

Figure 15-66 *IXIA System Components*



Chassis

The IxExplorer chassis holds IXIA module cards. The name or IP address of each chassis must be input; the type of the chassis is automatically discovered by the software. A chassis may hold any mix of module cards.

Card

The IxExplorer card corresponds to an IXIA load module card. The types of cards loaded in a chassis are automatically discovered and the appropriate number of ports is inserted into the hierarchy. Each port on a card has the same capabilities.

Port

The IxExplorer port corresponds to an individual port on an IXIA module card. Each port is independently programmed based on its ability to transmit and capture and its statistics capabilities. The IxExplorer software shows four separate views for programming and viewing operations:

- **Filters, statistics, and receive mode**—Sets the trigger and capture conditions for the capture buffer, the conditions for the four user-defined statistics, and the receive mode for the port.

- **Packet streams/flows**—Defines the streams within stream regions and the contents of packets.
- **Capture view**—Shows the data gathered during the capture operations. Data is displayed in raw form and interpreted for some protocols.
- **Statistics**—Shows the live statistics gathered during transmit and capture operation.

IxExplorer Windows

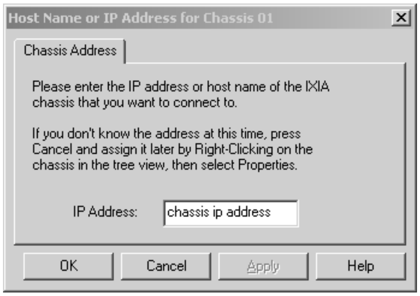
The main interface to the IxExplorer software and, therefore, the IXIA hardware, is through the many windows, dialogs, and tabs that IxExplorer displays. The following sections describe some of the basic components of IxExplorer:

- Main Window
- Explore Network Resources Window
- Capture View Window
- Statistic View Window
- Protocol Window

Main Window

After starting IxExplorer (by clicking on the **IxExplorer** icon or via the Start menu), a dialog box will appear asking for the address of the chassis, as shown in Figure 15-67.

Figure 15-67 *Chassis Address Dialog*



Host Name or IP Address for Chassis 01

Chassis Address

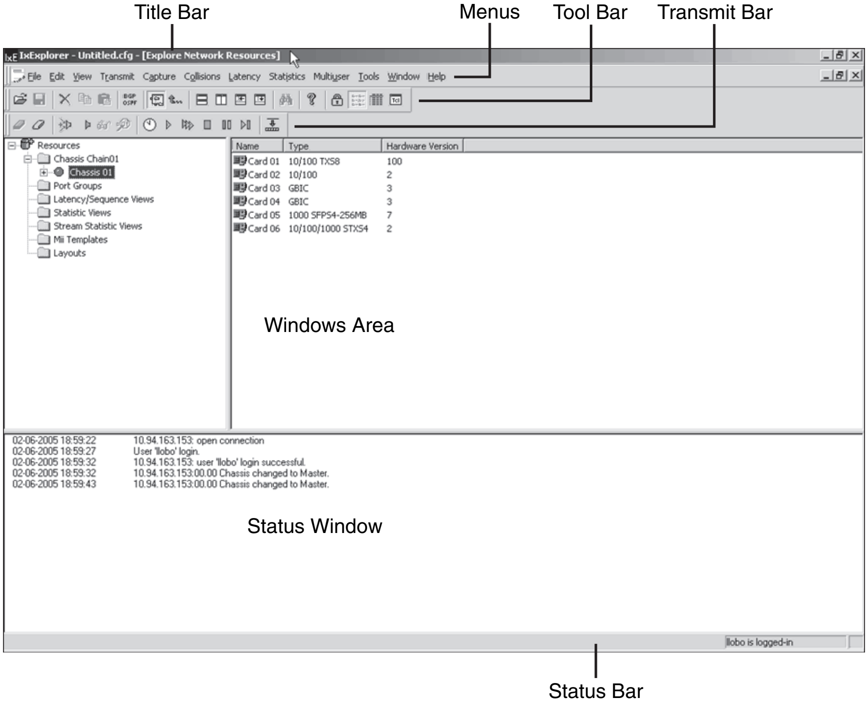
Please enter the IP address or host name of the IXIA chassis that you want to connect to.

If you don't know the address at this time, press Cancel and assign it later by Right-Clicking on the chassis in the tree view, then select Properties.

IP Address: chassis ip address

After entering the name of the chassis or its IP address, click **OK**. The IxExplorer main window will be displayed, as shown in Figure 15-68. The IxExplorer main window is the first window displayed when running IxExplorer, and the starting point for many operations. This window is opened initially only by clicking the **IxExplorer** icon or by selecting **IxExplorer** from the Start menu.

Figure 15-68 *Main Window*



Name	Type	Hardware Version
Card 01	10/100 TXS8	100
Card 02	10/100	2
Card 03	GBIC	3
Card 04	GBIC	3
Card 05	1000 SFPS4-256MB	7
Card 06	10/100/1000 STXS4	2

```
02-06-2005 18:59:22        10.94.163.153: open connection
02-06-2005 18:59:27        User 'llobo' login.
02-06-2005 18:59:32        10.94.163.153: user 'llobo' login successful.
02-06-2005 18:59:32        10.94.163.153:00.00 Chassis changed to Master.
02-06-2005 18:59:43        10.94.163.153:00.00 Chassis changed to Master.
```

The elements of the Basic IxExplorer window are described in Table 15-1.

Table 15-1 *Basic IxExplorer Window Elements*

Element	Description
Title Bar	Displays the name of the program plus the name of the workspace/configuration file in use.
Menu Bar	Location for the IxExplorer menus.
Toolbar	A standard Windows toolbar containing file, display, and help related icons.
Transmit Bar	An IXIA-specific toolbar that allows easy access to transmit and capture operations.
Windows Area	The bulk of the window accommodates one or more specific IxExplorer windows. These include • Explore Network Resources window • Capture View window • Latency/Sequence Checking View window • Statistic View window • Protocol window

Table 15-1 *Basic IxExplorer Window Elements (Continued)*

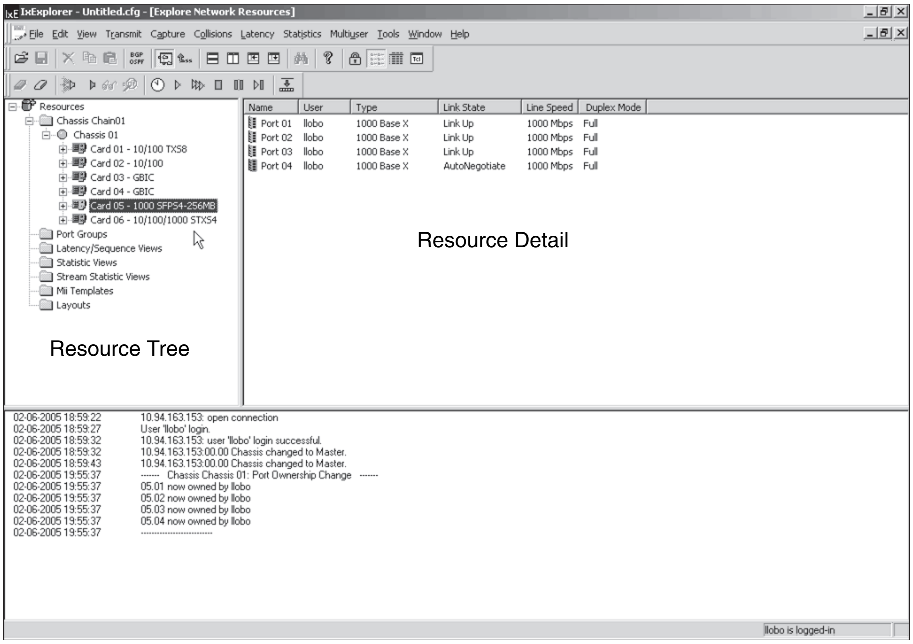
Element	Description
Status Window	Shows advisory messages sent from the server. Right-clicking in the window brings up a simple menu allowing the window to be cleared and the font for the window to be set.
Status Bar	Displays various status messages during IxExplorer operation.

Explore Network Resources Window

The Explore Network Resources window is located within the IxExplorer main window and shows the hierarchy of IXIA hardware resources on the left side of the window. The details view on the right side shows detailed information for the item selected in the left side.

An example of the Explore Network Resources window is shown in Figure 15-69.

Figure 15-69 *Network Resources Window Elements*



Name	User	Type	Link State	Line Speed	Duplex Mode
Port 01	llobo	1000 Base X	Link Up	1000 Mbps	Full
Port 02	llobo	1000 Base X	Link Up	1000 Mbps	Full
Port 03	llobo	1000 Base X	Link Up	1000 Mbps	Full
Port 04	llobo	1000 Base X	AutoNegotiate	1000 Mbps	Full

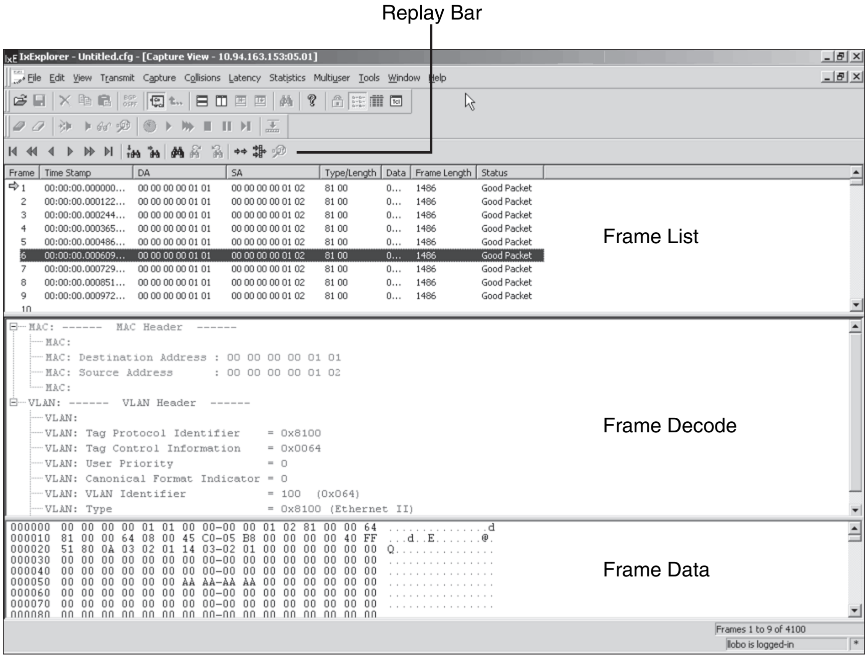
```
02-06-2005 18:59:22     10.94.163.153: open connection
02-06-2005 18:59:27     User 'llobo' login.
02-06-2005 18:59:32     10.94.163.153: user 'llobo' login successful.
02-06-2005 18:59:32     10.94.163.153:00.00 Chassis changed to Master.
02-06-2005 18:59:43     10.94.163.153:00.00 Chassis changed to Master.
02-06-2005 19:55:37     -------  Chassis Chassis 01: Port Ownership Change  -------
02-06-2005 19:55:37     05.01 now owned by llobo
02-06-2005 19:55:37     05.02 now owned by llobo
02-06-2005 19:55:37     05.03 now owned by llobo
02-06-2005 19:55:37     05.04 now owned by llobo
02-06-2005 19:55:37     -------------------------
```

The Explore Network Resources window is where most setup and programming of IXIA hardware is performed. The left side of the display holds a tree, which consists of the IXIA architecture hierarchy, from Chassis Chain down to Port level. For any item selected on the left side, the right side of the screen shows details for the selected item. This is sometimes a listing of contained items, and sometimes an active display, as in the Statistic View.

Capture View Window

The Capture View window is used to look at the data recorded from the DUT. The Capture View is accessed by selecting a port in the Resource tree, and then double-clicking **Capture View** from the list of options in the Resource details view. An example of the Capture View window is shown in Figure 15-70.

Figure 15-70 *Capture View Window*



Frame	Time Stamp	DA	SA	Type/Length	Data	Frame Length	Status
1	00:00:00.000000...	00 00 00 00 01 01	00 00 00 00 01 02	81 00	0...	1486	Good Packet
2	00:00:00.000122...	00 00 00 00 01 01	00 00 00 00 01 02	81 00	0...	1486	Good Packet
3	00:00:00.000244...	00 00 00 00 01 01	00 00 00 00 01 02	81 00	0...	1486	Good Packet
4	00:00:00.000365...	00 00 00 00 01 01	00 00 00 00 01 02	81 00	0...	1486	Good Packet
5	00:00:00.000486...	00 00 00 00 01 01	00 00 00 00 01 02	81 00	0...	1486	Good Packet
6	00:00:00.000609...	00 00 00 00 01 01	00 00 00 00 01 02	81 00	0...	1486	Good Packet
7	00:00:00.000729...	00 00 00 00 01 01	00 00 00 00 01 02	81 00	0...	1486	Good Packet
8	00:00:00.000851...	00 00 00 00 01 01	00 00 00 00 01 02	81 00	0...	1486	Good Packet
9	00:00:00.000972...	00 00 00 00 01 01	00 00 00 00 01 02	81 00	0...	1486	Good Packet
10							

```
MAC: ------  MAC Header  ------
  MAC:
  MAC: Destination Address : 00 00 00 00 01 01
  MAC: Source Address      : 00 00 00 00 01 02
  MAC:
VLAN: ------  VLAN Header  ------
  VLAN:
  VLAN: Tag Protocol Identifier    = 0x8100
  VLAN: Tag Control Information    = 0x0064
  VLAN: User Priority              = 0
  VLAN: Canonical Format Indicator = 0
  VLAN: VLAN Identifier            = 100  (0x064)
  VLAN: Type                       = 0x8100 (Ethernet II)
```

```
000000  00 00 00 00 01 01 00 00-00 00 01 02 81 00 00 64  ...............d
000010  81 00 00 64 08 00 45 C0-05 B8 00 00 00 00 40 FF  ...d..E.......@.
000020  51 80 0A 03 02 01 14 03-02 01 00 00 00 00 00 00  Q...............
000030  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
000040  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
000050  00 00 00 00 00 00 AA AA-AA AA 00 00 00 00 00 00  ................
000060  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
000070  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
000080  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
```

The elements of the Capture View window are described in Table 15-2.

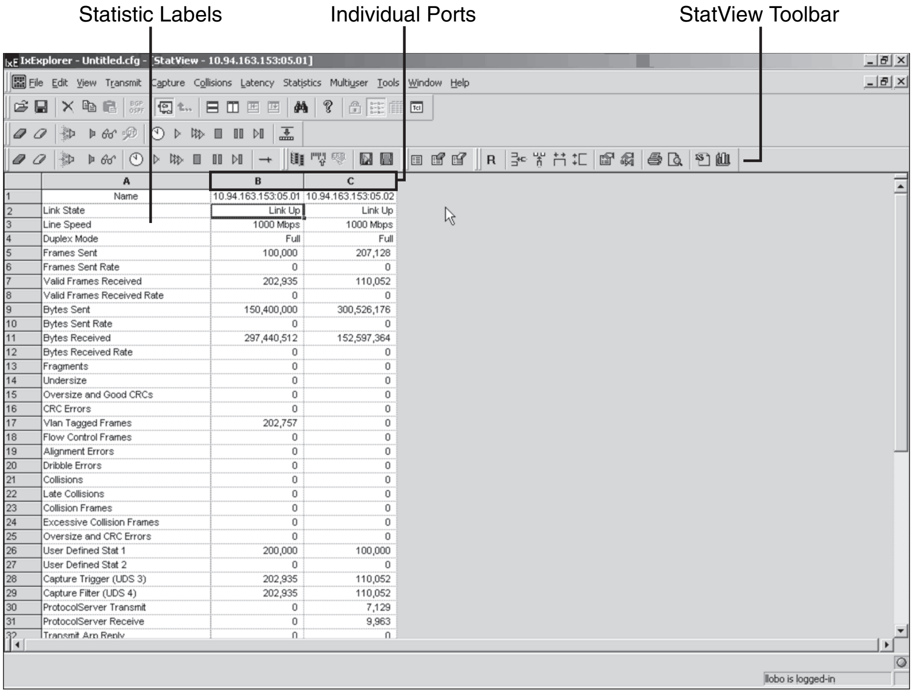
Table 15-2 *Capture View Window Elements*

Element	Description
Replay Bar	A special toolbar used to scan captured frames.
Frame List	Lists a page of the frames that are present in the capture buffer for a port.
Frame Decode	Displays an attempt to decode the frame, in terms of protocol-dependent parameters.
Frame Data	Displays the raw data (in hexadecimal format) for the frame.

Statistic View Window

Statistic Views are used to monitor various statistics for a single port or a group of ports. A new Statistic View is opened by right-clicking the **Statistic Views** in the Resource tree, then selecting the **New** option from the menu. An existing Statistic View is opened by selecting **Statistic Views** in the Resource tree, then double-clicking one of the saved views from the Resource detail display. An example of the Statistic View window is shown in Figure 15-71.

Figure 15-71 *Statistic View Window Elements*


Statistic Labels
Individual Ports
StatView Toolbar
IxExplorer - Untitled.cfg - [StatView - 10.94.163.153:05.01]
File Edit View Transmit Capture Collisions Latency Statistics Multiuser Tools Window Help
llobo is logged-in

	A	B	C
1	Name	10.94.163.153:05.01	10.94.163.153:05.02
2	Link State	Link Up	Link Up
3	Line Speed	1000 Mbps	1000 Mbps
4	Duplex Mode	Full	Full
5	Frames Sent	100,000	207,128
6	Frames Sent Rate	0	0
7	Valid Frames Received	202,935	110,052
8	Valid Frames Received Rate	0	0
9	Bytes Sent	150,400,000	300,526,176
10	Bytes Sent Rate	0	0
11	Bytes Received	297,440,512	152,597,364
12	Bytes Received Rate	0	0
13	Fragments	0	0
14	Undersize	0	0
15	Oversize and Good CRCs	0	0
16	CRC Errors	0	0
17	Vlan Tagged Frames	202,757	0
18	Flow Control Frames	0	0
19	Alignment Errors	0	0
20	Dribble Errors	0	0
21	Collisions	0	0
22	Late Collisions	0	0
23	Collision Frames	0	0
24	Excessive Collision Frames	0	0
25	Oversize and CRC Errors	0	0
26	User Defined Stat 1	200,000	100,000
27	User Defined Stat 2	0	0
28	Capture Trigger (UDS 3)	202,935	110,052
29	Capture Filter (UDS 4)	202,935	110,052
30	ProtocolServer Transmit	0	7,129
31	ProtocolServer Receive	0	9,963
32	Transmit Arp Reply	0	0

The elements of the Statistic View window are described in Table 15-3.

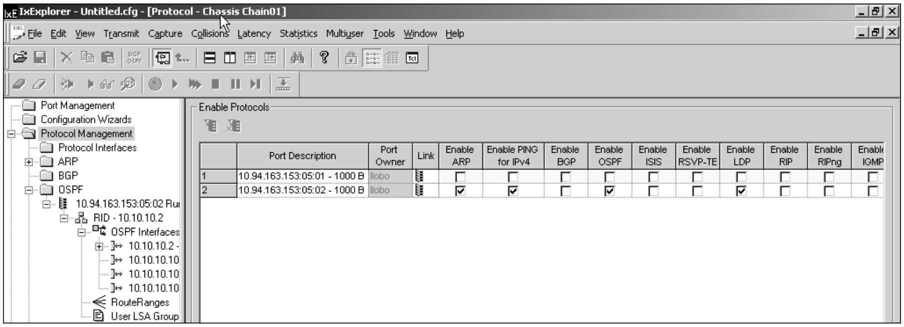
Table 15-3 *Elements of the Statistic View Window*

Element	Description
StatView Toolbar	A custom toolbar used to control transmit, capture, and statistics operations.
Statistic Labels	The labels for each of the rows of the display. These are the statistics chosen for the set of ports in a statistics group.
Individual Ports	The column headings show the individual ports that are a part of the statistics group.

Protocol Window

The Protocol window allows configuration of routing protocols including BGP, OSPF, IS-IS, RSVP-TE, LDP, RIP, RIPng, IGMP, and PIM-SM, as shown in Figure 15-72. Note that the Protocol window is named as IXRouter in IXIA software versions 4.0 and higher.

Figure 15-72 *Protocol Select Window*



	Port Description	Port Owner	Link	Enable ARP	Enable PING for IPv4	Enable BGP	Enable OSPF	Enable ISIS	Enable RSVP-TE	Enable LDP	Enable RIP	Enable RIPng	Enable IGMP
1	10.94.163.153:05:01 - 1000 B	llobo		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2	10.94.163.153:05:02 - 1000 B	llobo		☑	☑	☐	☑	☐	☐	☑	☐	☐	☐

The fields and controls in the main Protocol window (showing protocol selections) are described in Table 15-4.

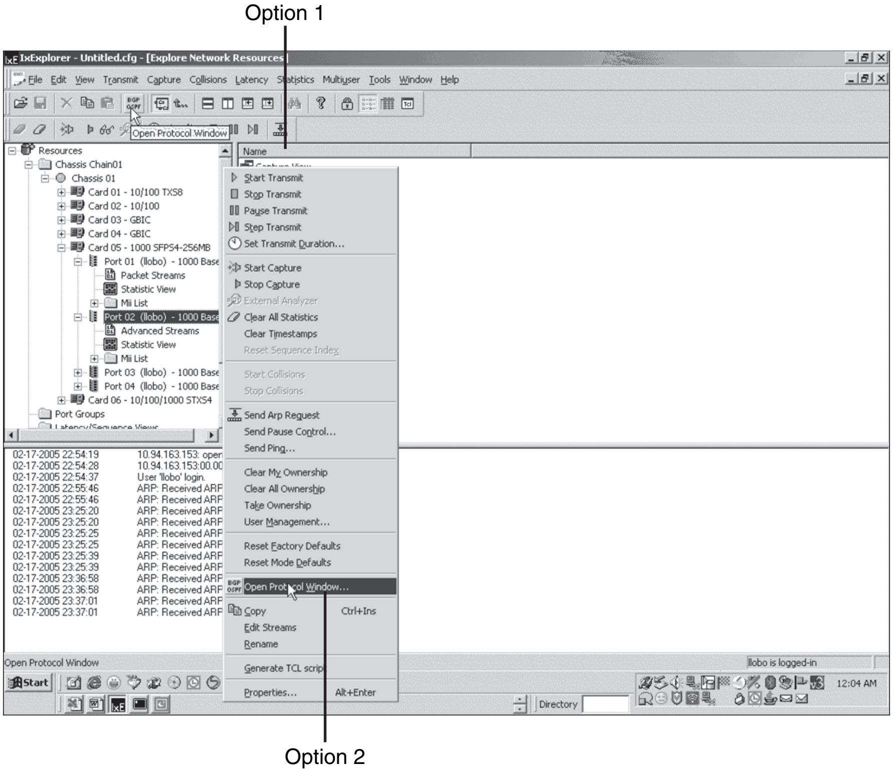
Table 15-4 *Protocol Window Elements*

Field/Control	Description
List of Protocols	A tree structure that presents the protocols and access to various levels of configuration windows, depending on the protocol selected.
Port Selection Window	The window where protocols are selected for use with available ports. The protocols in the grid are grayed out for ports that do not support those protocols.

To go the Protocol window, there are two options:

- **Option 1**—Click the **Protocol Window** icon on the IxExplorer toolbar, as shown in Figure 15-73.
- **Option 2**—Right-click **Chassis** or **Card** in the Resource tree located in the window area, as shown in Figure 15-73.

Figure 15-73 *Steps to Protocol Select Window*



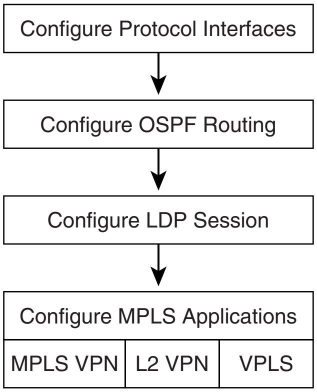
```
02-17-2005 22:54:19        10.94.163.153: open
02-17-2005 22:54:28        10.94.163.153:00.00
02-17-2005 22:54:37        User 'llobo' login.
02-17-2005 22:55:46        ARP: Received ARP
02-17-2005 22:55:46        ARP: Received ARP
02-17-2005 23:25:20        ARP: Received ARP
02-17-2005 23:25:20        ARP: Received ARP
02-17-2005 23:25:25        ARP: Received ARP
02-17-2005 23:25:25        ARP: Received ARP
02-17-2005 23:25:39        ARP: Received ARP
02-17-2005 23:25:39        ARP: Received ARP
02-17-2005 23:36:58        ARP: Received ARP
02-17-2005 23:36:58        ARP: Received ARP
02-17-2005 23:37:01        ARP: Received ARP
02-17-2005 23:37:01        ARP: Received ARP
```

Basic MPLS Configuration Procedure on IXIA

Figure 15-74 shows the IXIA configuration flowchart. The following three steps in the flowchart are mandatory and are a prerequisite to test all MPLS applications shown in Step 4:

- Configure protocol interfaces
- Configure OSPF routing
- Configure LDP session

Figure 15-74 *IXIA Configuration Flowchart*

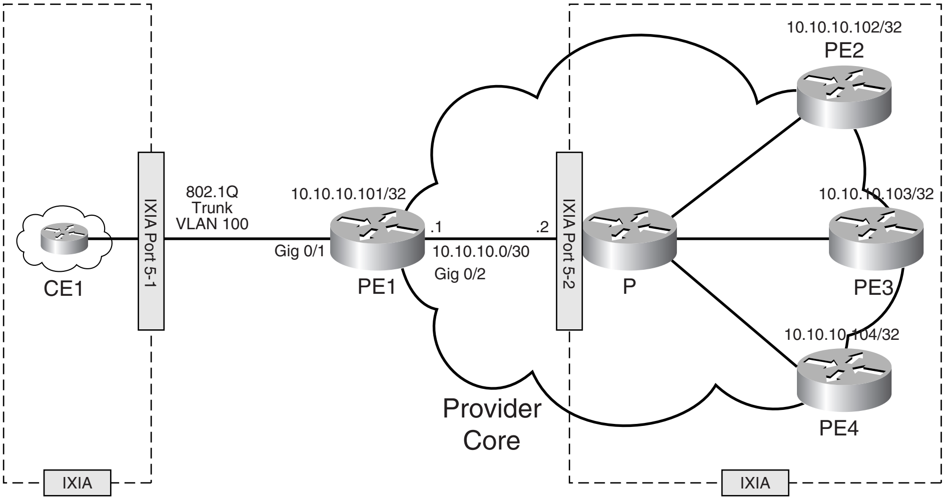


The following sections explore these steps in greater detail.

Configure Protocol Interfaces

Figure 15-75 illustrates an MPLS test network where PE1 is the DUT. PE1 Port GIG0/1 serves as a CE interface and connects to IXIA Card 5, Port 1, which functions as a CE device. PE1 Port Gig0/2 serves as a provider interface and connects to IXIA Card 5, Port 2, which emulates the provider Router P, and PE Routers PE2, PE3, and PE4.

Figure 15-75 *MPLS Provider Network*



The steps to create an interface on the IXIA are as follows:

Step 1 Go to the Protocol window. In the Protocol window, perform the following steps, as shown in Figure 15-76:

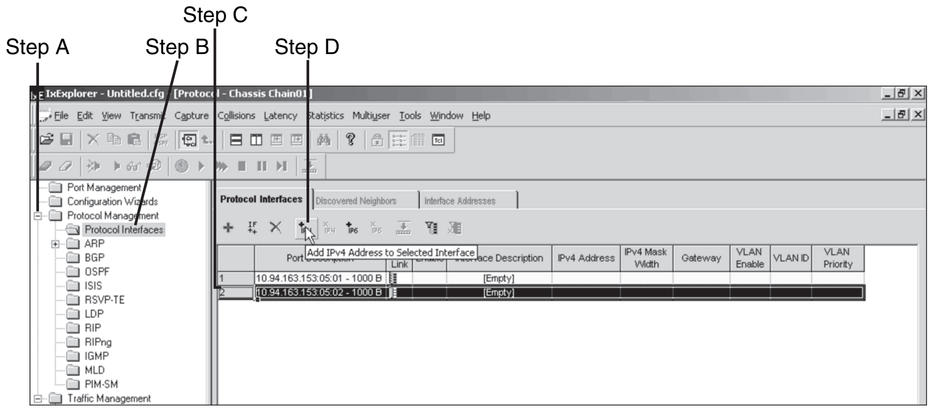
Step A—Expand the Protocol Management folder.

Step B—Select the Protocol Interfaces.

Step C—Select the second interface.

Step D—Click the **Add IPv4 Address to Selected Interface**.

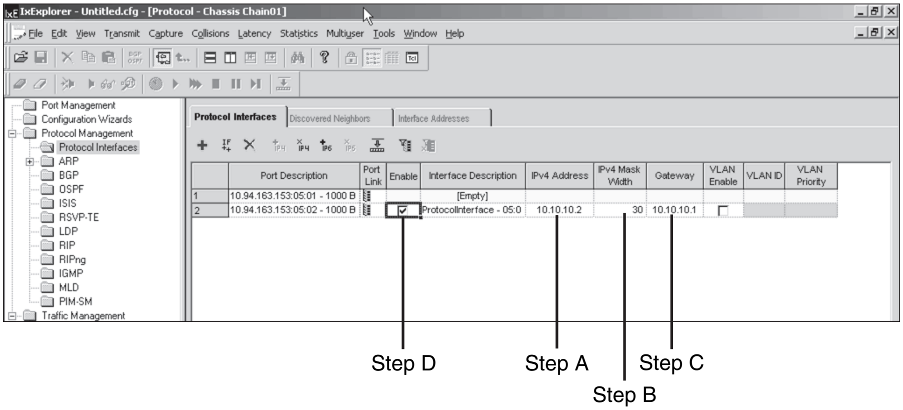
Figure 15-76 *Protocol Interfaces*



	Port	Link		ace Description	IPv4 Address	IPv4 Mask Width	Gateway	VLAN Enable	VLAN ID	VLAN Priority
1	10.94.163.153:05:01 - 1000 B			[Empty]						
2	10.94.163.153:05:02 - 1000 B			[Empty]						

Step 2 This step is shown in Figure 15-77.

Figure 15-77 *Configure P Router Interface*



	Port Description	Port Link	Enable	Interface Description	IPv4 Address	IPv4 Mask Width	Gateway	VLAN Enable	VLAN ID	VLAN Priority
1	10.94.163.153:05:01 - 1000 B			[Empty]						
2	10.94.163.153:05:02 - 1000 B		☑	ProtocolInterface - 05:0	10.10.10.2	30	10.10.10.1	☐		

Step A—Configure the IP address 10.10.10.2 for the interface. This is the P router interface connected to the DUT's PE1 provider interface (10.10.10.1/30).

Step B—Configure the IP address mask.

Step C—Configure the gateway IP address, 10.10.10.1.

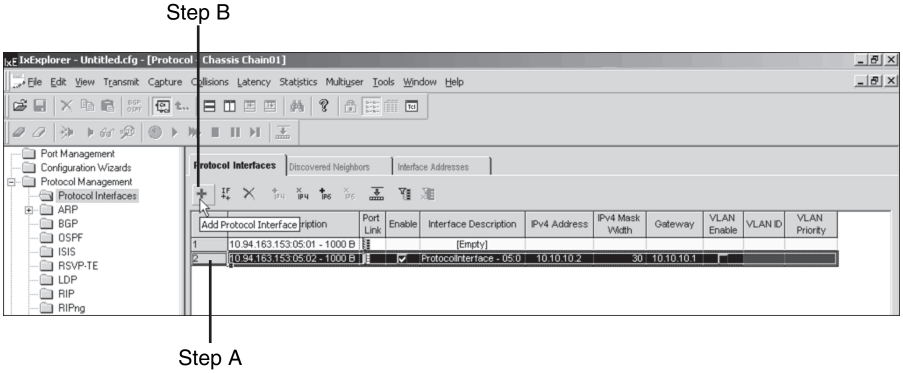
Step D—Enable the interface.

Step 3 In this step, additional interfaces or loopback interfaces are added on each of the emulated provider Routers PE2, PE3, and PE4:

Step A—Select the second interface, as shown in Figure 15-78.

Step B—Click **Add Protocol Interface** three times so that three additional interfaces can be configured.

Figure 15-78 *Configure Loopback Interfaces for PE Routers PE2, PE3, and PE4*



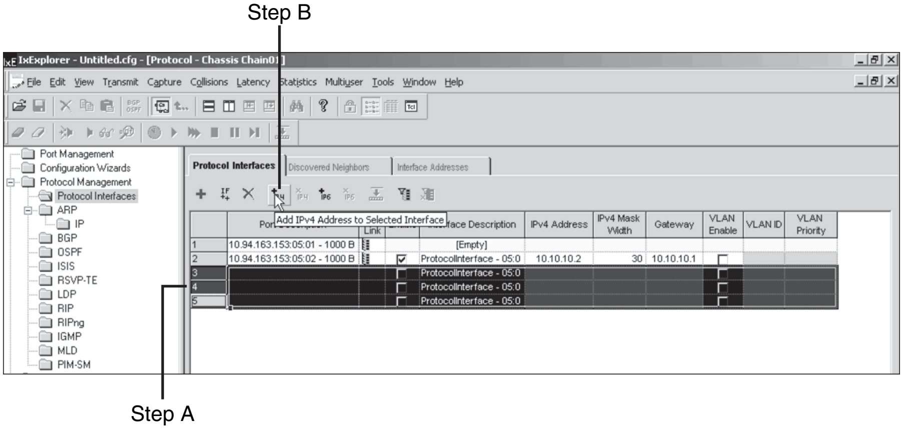
	…ription	Port Link	Enable	Interface Description	IPv4 Address	IPv4 Mask Width	Gateway	VLAN Enable	VLAN ID	VLAN Priority
1	10.94.163.153:05:01 - 1000 B			[Empty]						
2	10.94.163.153:05:02 - 1000 B		☑	ProtocolInterface - 05:0	10.10.10.2	30	10.10.10.1	☐		

Step 4 This step is shown in Figure 15-79:

Step A—In this step, select the three additional interfaces created in Step 3.

Step B—Click **Add IPv4 Address to Selected Interface**.

Figure 15-79 *Configuring IPv4 Address for Additional Interfaces*



	Por…	…Link		…face Description	IPv4 Address	IPv4 Mask Width	Gateway	VLAN Enable	VLAN ID	VLAN Priority
1	10.94.163.153:05:01 - 1000 B			[Empty]						
2	10.94.163.153:05:02 - 1000 B		☑	ProtocolInterface - 05:0	10.10.10.2	30	10.10.10.1	☐		
3			☐	ProtocolInterface - 05:0				☐		
4			☐	ProtocolInterface - 05:0				☐		
5			☐	ProtocolInterface - 05:0				☐		

Step 5 This step is shown in Figure 15-80:

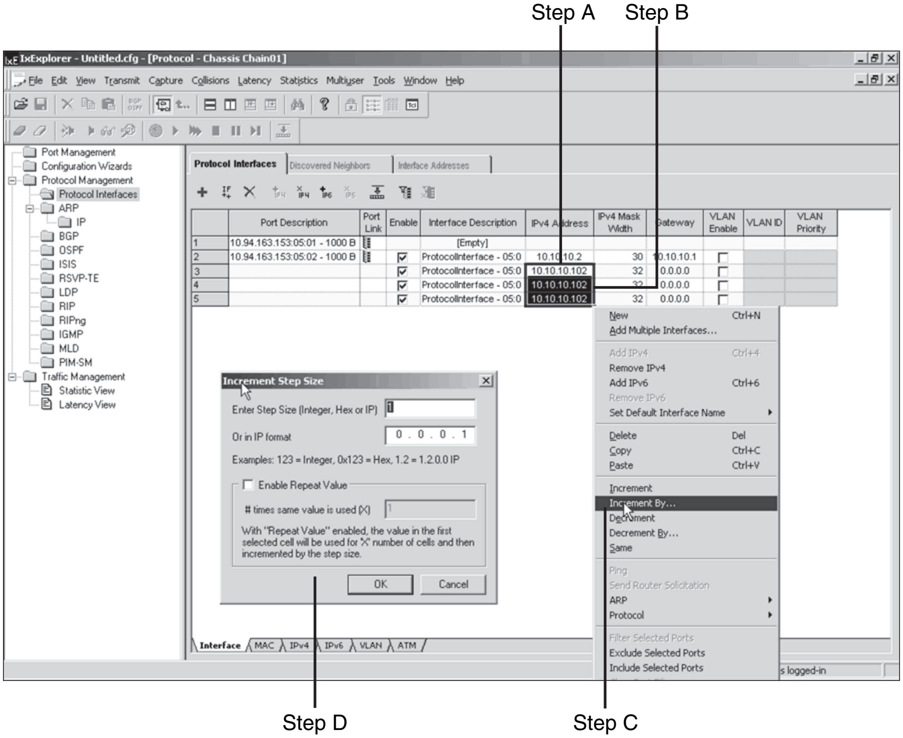
Step A—Type **10.10.10.102** in the IPv4 field.

Step B—Select the cell with the value 10.10.10.102 and drag the fill handle across the cells you want to fill, and then release the mouse button. (The fill handle is the small black square in the lower-right corner of the selection. When you point to the fill handle, the pointer changes to a black cross.)

Step C—Right-click the mouse and go to Increment By Option, as shown in Figure 15-80. Click **Increment By**.

Step D—You will be in the Increment Step Size dialog box. By default, the last octet is shown to be incremented. Click **OK** and you will see the output shown in Figure 15-81.

Figure 15-80 *Configuring IPv4 Addresses for PE2, PE3, and PE4*



	Port Description	Port Link	Enable	Interface Description	IPv4 Address	IPv4 Mask Width	Gateway	VLAN Enable	VLAN ID	VLAN Priority
1	10.94.163.153:05:01 - 1000 B			[Empty]						
2	10.94.163.153:05:02 - 1000 B		☑	ProtocolInterface - 05:0	10.10.10.2	30	10.10.10.1	☐		
3			☑	ProtocolInterface - 05:0	10.10.10.102	32	0.0.0.0	☐		
4			☑	ProtocolInterface - 05:0	10.10.10.102	32	0.0.0.0	☐		
5			☑	ProtocolInterface - 05:0	10.10.10.102	32	0.0.0.0	☐		

Increment Step Size

Enter Step Size (Integer, Hex or IP): 1

Or in IP format: 0 . 0 . 0 . 1

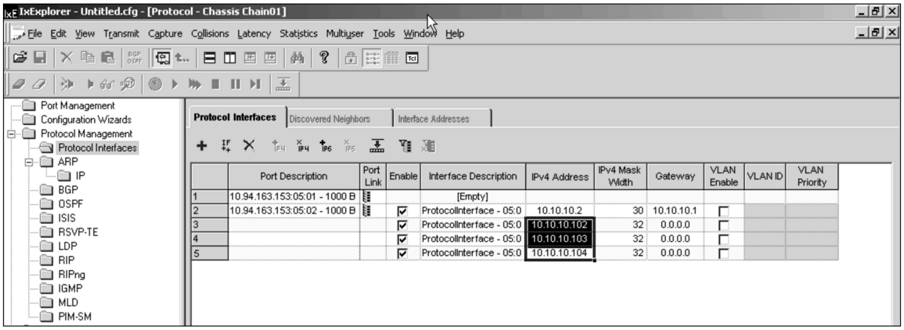
Examples: 123 = Integer, 0x123 = Hex, 1.2 = 1.2.0.0 IP

☐ Enable Repeat Value

times same value is used (X): 1

With "Repeat Value" enabled, the value in the first selected cell will be used for "X" number of cells and then incremented by the step size.

Figure 15-81 *Output for PE2, PE3, and PE4 IP Addresses*



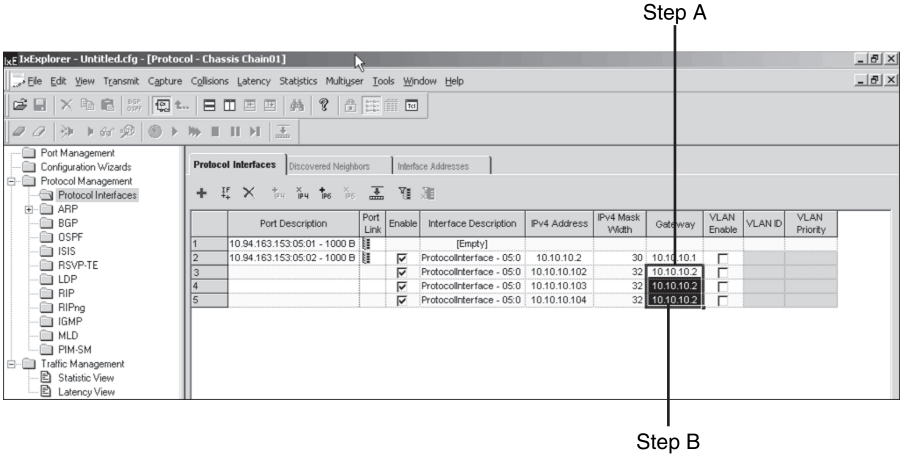
	Port Description	Port Link	Enable	Interface Description	IPv4 Address	IPv4 Mask Width	Gateway	VLAN Enable	VLAN ID	VLAN Priority
1	10.94.163.153:05:01 - 1000 B			[Empty]						
2	10.94.163.153:05:02 - 1000 B		☑	ProtocolInterface - 05:0	10.10.10.2	30	10.10.10.1	☐		
3			☑	ProtocolInterface - 05:0	10.10.10.102	32	0.0.0.0	☐		
4			☑	ProtocolInterface - 05:0	10.10.10.103	32	0.0.0.0	☐		
5			☑	ProtocolInterface - 05:0	10.10.10.104	32	0.0.0.0	☐		

Step 6 This step is shown in Figure 15-82:

Step A—Type **10.10.10.2** in the gateway field for the PE router with IP address 10.10.10.102.

Step B—Select the gateway cell for 10.10.10.102 and drag the fill handle across the cells you want to fill, and then release the mouse button.

Figure 15-82 *Configure the Gateway Address for PE2, PE3, and PE4*



	Port Description	Port Link	Enable	Interface Description	IPv4 Address	IPv4 Mask Width	Gateway	VLAN Enable	VLAN ID	VLAN Priority
1	10.94.163.153:05:01 - 1000 B			[Empty]						
2	10.94.163.153:05:02 - 1000 B		☑	ProtocolInterface - 05:0	10.10.10.2	30	10.10.10.1	☐		
3			☑	ProtocolInterface - 05:0	10.10.10.102	32	10.10.10.2	☐		
4			☑	ProtocolInterface - 05:0	10.10.10.103	32	10.10.10.2	☐		
5			☑	ProtocolInterface - 05:0	10.10.10.104	32	10.10.10.2	☐		

Configure and Verify OSPF in the Provider Core on IXIA

The steps to configure OSPF routing on IXIA are as follows:

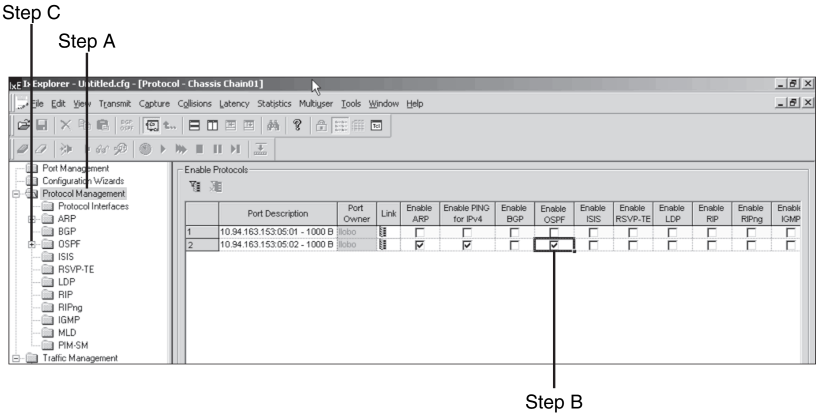
Step 1 In the Protocol window, as shown in Figure 15-83,

Step A—Select the **Protocol Management** folder by clicking it.

Step B—Enable the checkbox marked OSPF.

Step C—Expand OSPF.

Figure 15-83 *Enable OSPF*



	Port Description	Port Owner	Link	Enable ARP	Enable PING for IPv4	Enable BGP	Enable OSPF	Enable ISIS	Enable RSVP-TE	Enable LDP	Enable RIP	Enable RIPng	Enable IGMP
1	10.94.163.153:05:01 - 1000 B	Ilobo		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2	10.94.163.153:05:02 - 1000 B	Ilobo		☑	☑	☐	☑	☐	☐	☐	☐	☐	☐

Step 2 As shown in Figure 15-84,

Step A—Under the OSPF node in the Protocol window, expand the tree and select the card port designation. In the example, Card 5, Port 2 is used.

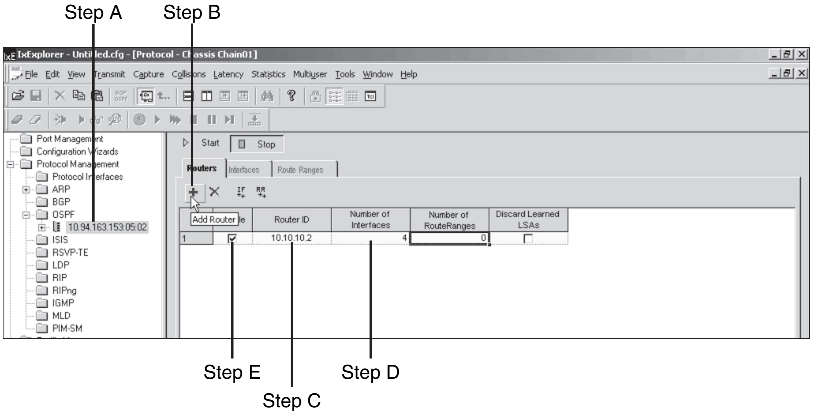
Step B—Add the OSPF router by clicking the "plus" icon titled **Add Router**.

Step C—Configure the OSPF router ID 10.10.10.2.

Step D—Configure the number of interfaces, in this case 2; the first interface is the one directly connected to the DUT. This interface is emulating the P router (10.10.10.2) and serves as a gateway to the emulated PEs (PE2, PE3, and PE4) and the MPLS cloud. The second interface is the emulated PE router and, in this case, you would create PE2 (10.10.10.102).

Step E—Finally, enable the OSPF router.

Figure 15-84 *Create OSPF Router*



	Enable	Router ID	Number of Interfaces	Number of RouteRanges	Discard Learned LSAs
1	☑	10.10.10.2	4	0	☐

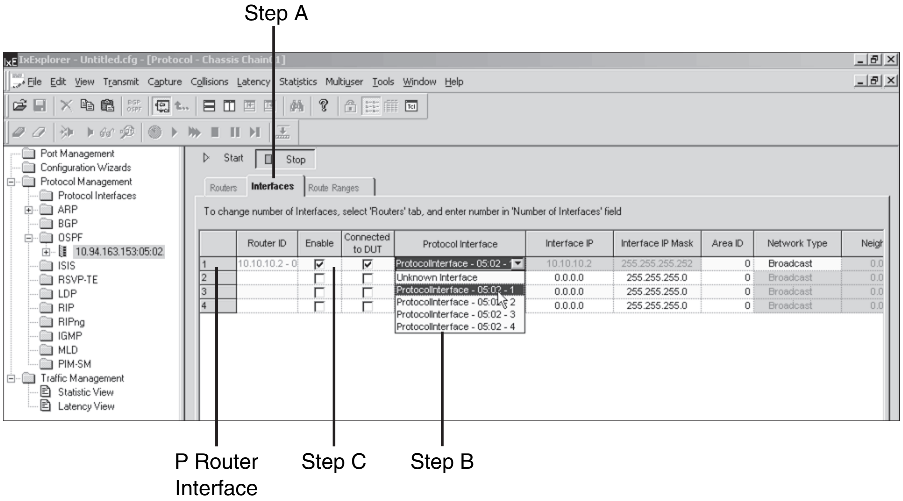
Step 3 As shown in Figure 15-85,

Step A—Click the **Interfaces** tab as shown in Figure 15-85.

Step B—Select the protocol interface, in this case (ProtocolInterface—05:02-1), which should be the 10.10.10.2 interface.

Step C —Enable the P router interface. Ensure that this network type is configured for broadcast.

Figure 15-85 *Enable OSPF on P Router Interface*



To change number of Interfaces, select 'Routers' tab, and enter number in 'Number of Interfaces' field

	Router ID	Enable	Connected to DUT	Protocol Interface	Interface IP	Interface IP Mask	Area ID	Network Type	Neigh
1	10.10.10.2 - 0	☑	☑	ProtocolInterface - 05:02 - 1	10.10.10.2	255.255.255.252	0	Broadcast	0.0
2		☐	☐		0.0.0.0	255.255.255.0	0	Broadcast	0.0
3		☐	☐		0.0.0.0	255.255.255.0	0	Broadcast	0.0
4		☐	☐		0.0.0.0	255.255.255.0	0	Broadcast	0.0

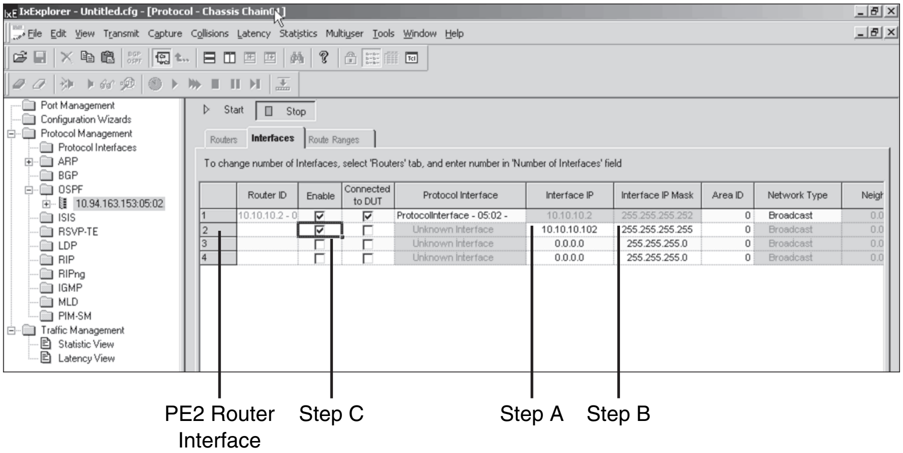
Step 4 As shown in Figure 15-86, configure the PE2 router interface:

Step A—Configure the interface IP address to 10.10.10.102.

Step B—Configure the mask, in this case 255.255.255.255.

Step C—Enable the PE2 router interface. Note that this is not a connected interface, so do not check the Connected to DUT box.

Figure 15-86 *Enable OSPF on PE2 Router Interface*

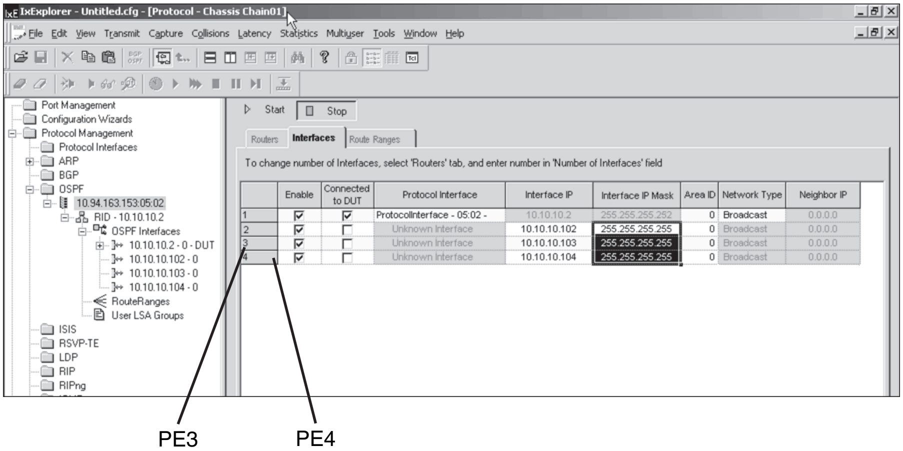


To change number of Interfaces, select 'Routers' tab, and enter number in 'Number of Interfaces' field

	Router ID	Enable	Connected to DUT	Protocol Interface	Interface IP	Interface IP Mask	Area ID	Network Type	Neigh
1	10.10.10.2 - 0	☑	☑	ProtocolInterface - 05:02 -	10.10.10.2	255.255.255.252	0	Broadcast	0.0
2		☑	☐	Unknown Interface	10.10.10.102	255.255.255.255	0	Broadcast	0.0
3		☐	☐	Unknown Interface	0.0.0.0	255.255.255.0	0	Broadcast	0.0
4		☐	☐	Unknown Interface	0.0.0.0	255.255.255.0	0	Broadcast	0.0

Step 5 As shown in Figure 15-87, enable OSPF on PE3 and PE4 router interfaces.

Figure 15-87 *Enable OSPF on PE2, PE3, and PE4 Router Interfaces*



To change number of Interfaces, select 'Routers' tab, and enter number in 'Number of Interfaces' field

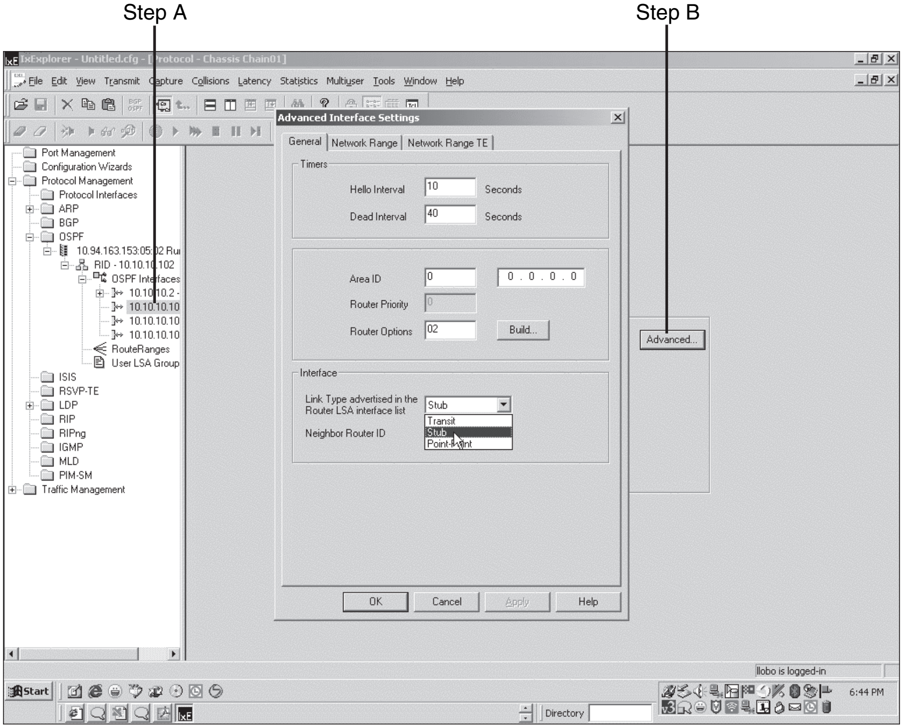
	Enable	Connected to DUT	Protocol Interface	Interface IP	Interface IP Mask	Area ID	Network Type	Neighbor IP
1	☑	☑	ProtocolInterface - 05:02 -	10.10.10.2	255.255.255.252	0	Broadcast	0.0.0.0
2	☑	☐	Unknown Interface	10.10.10.102	255.255.255.255	0	Broadcast	0.0.0.0
3	☑	☐	Unknown Interface	10.10.10.103	255.255.255.255	0	Broadcast	0.0.0.0
4	☑	☐	Unknown Interface	10.10.10.104	255.255.255.255	0	Broadcast	0.0.0.0

Step 6 Select the PE2 interface. Double-click this interface to get to the screen shown in Figure 15-88:

Step A—Change the link type for the router LSA to be generated as a stub.

Step B—Double-click **Advanced** and change the link type to be a stub; click **OK** (not depicted).

Figure 15-88 *OSPF Configuration Settings*



Hello Interval: 10 Seconds

Dead Interval: 40 Seconds

Area ID: 0 — 0 . 0 . 0 . 0

Router Priority: 0

Router Options: 02

Link Type advertised in the Router LSA interface list: Stub

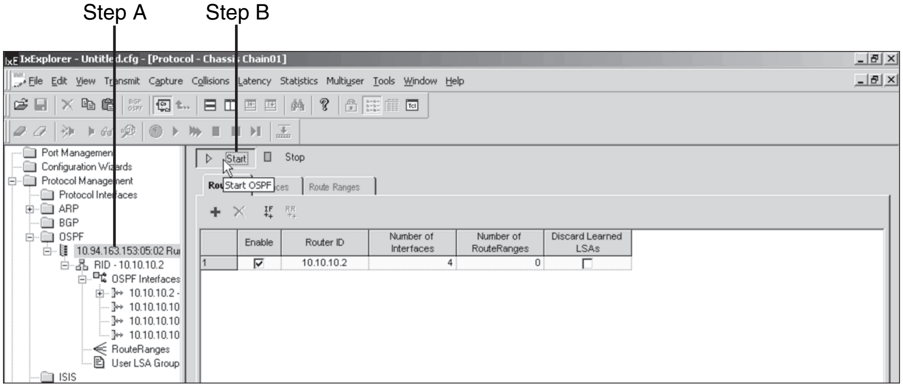
Neighbor Router ID:

Step 7 As shown in Figure 15-89,

Step A—Click the interface card, as shown in Figure 15-89.

Step B—Start the OSPF process by clicking the **Start** icon.

Figure 15-89 *Start OSPF Process*

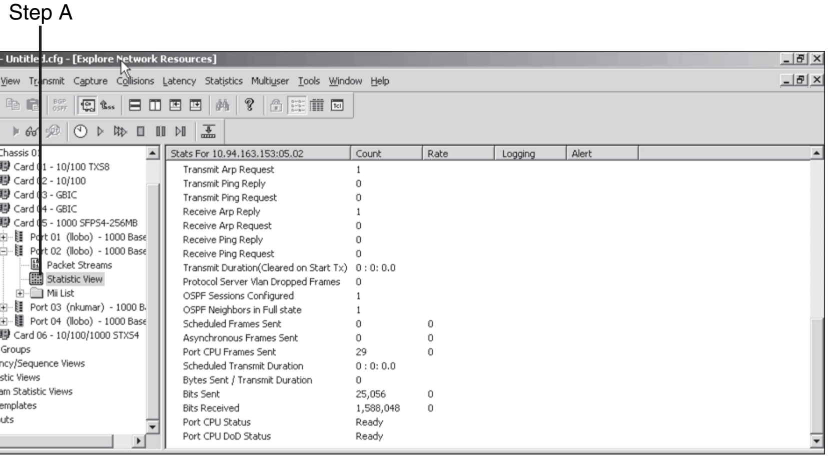


	Enable	Router ID	Number of Interfaces	Number of RouteRanges	Discard Learned LSAs
1	☑	10.10.10.2	4	0	☐

Step 8 To verify OSPF connections, go to the **Windows** tab and click **Explore Network Resources**. Then, follow the steps shown in Figure 15-90:

Step A—Click **Statistic View**, as shown in Figure 15-90. On the right pane, look at **OSPF Session Configured** and **OSPF Neighbors in Full State**.

Figure 15-90 *OSPF Verification*


Step A
IxExplorer - Untitled.cfg - [Explore Network Resources]
File Edit View Transmit Capture Collisions Latency Statistics Multiuser Tools Window Help
Chassis 01
Card 01 - 10/100 TXS8
Card 02 - 10/100
Card 03 - GBIC
Card 04 - GBIC
Card 05 - 1000 SFPS4-256MB
Port 01 (llobo) - 1000 Base
Port 02 (llobo) - 1000 Base
Packet Streams
Statistic View
Mii List
Port 03 (nkumar) - 1000 B.
Port 04 (llobo) - 1000 Base
Card 06 - 10/100/1000 STXS4
Port Groups
Latency/Sequence Views
Statistic Views
Stream Statistic Views
Mii Templates
Layouts

Stats For 10.94.163.153:05.02	Count	Rate	Logging	Alert
Transmit Arp Request	1			
Transmit Ping Reply	0			
Transmit Ping Request	0			
Receive Arp Reply	1			
Receive Arp Request	0			
Receive Ping Reply	0			
Receive Ping Request	0			
Transmit Duration(Cleared on Start Tx)	0 : 0: 0.0			
Protocol Server Vlan Dropped Frames	0			
OSPF Sessions Configured	1			
OSPF Neighbors in Full state	1			
Scheduled Frames Sent	0	0		
Asynchronous Frames Sent	0	0		
Port CPU Frames Sent	29	0		
Scheduled Transmit Duration	0 : 0: 0.0			
Bytes Sent / Transmit Duration	0			
Bits Sent	25,056	0		
Bits Received	1,588,048	0		
Port CPU Status	Ready			
Port CPU DoD Status	Ready			

On the DUT, issue a **show ip ospf neighbor** to verify the OSPF connectivity between the DUT and IXIA Port 5-2. This is shown in Example 15-11.

Example 15-11 **show ip ospf neighbor** *on PE1*

```
PE1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.10.2        0   FULL/DROTHER    00:00:34    10.10.10.2      GE-WAN3/3
```

Configure and Verify LDP in Provider Core on IXIA

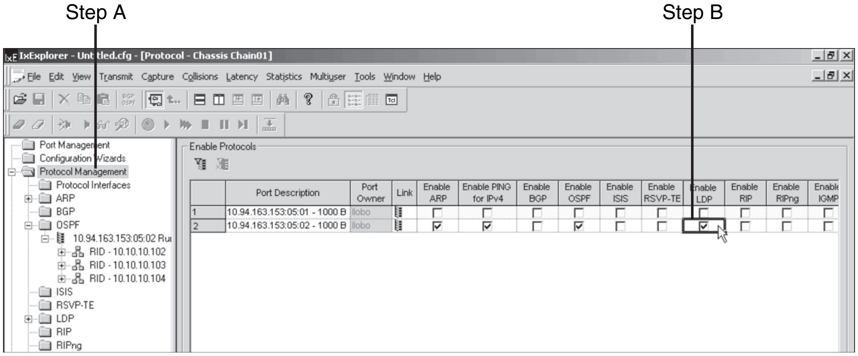
This section outlines the steps taken to implement LDP with the emulated provider core routers between the IXIA and the DUT:

Step 1 In the IxExplorer window, open the Protocol window by clicking on a chassis, card, or port and then clicking on the Protocol Window icon:

Step A—Once in the Protocol window, click the **Protocol Management** folder, as shown in Figure 15-91.

Step B—Enable LDP emulation on Port 05:01, as shown in Figure 15-91.

Figure 15-91 *Enable LDP on the IXIA Interface*



	Port Description	Port Owner	Link	Enable ARP	Enable PING for IPv4	Enable BGP	Enable OSPF	Enable ISIS	Enable RSVP-TE	Enable LDP	Enable RIP	Enable RIPng	Enable IGMP
1	10.94.163.153:05:01 - 1000 B	llobo		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2	10.94.163.153:05:02 - 1000 B	llobo		☑	☑	☐	☑	☐	☐	☑	☐	☐	☐

Step 2 The steps to add LDP routers are

Step A—Click the **LDP** folder.

Step B—Click the **Routers** tab, as shown in Figure 15-92.

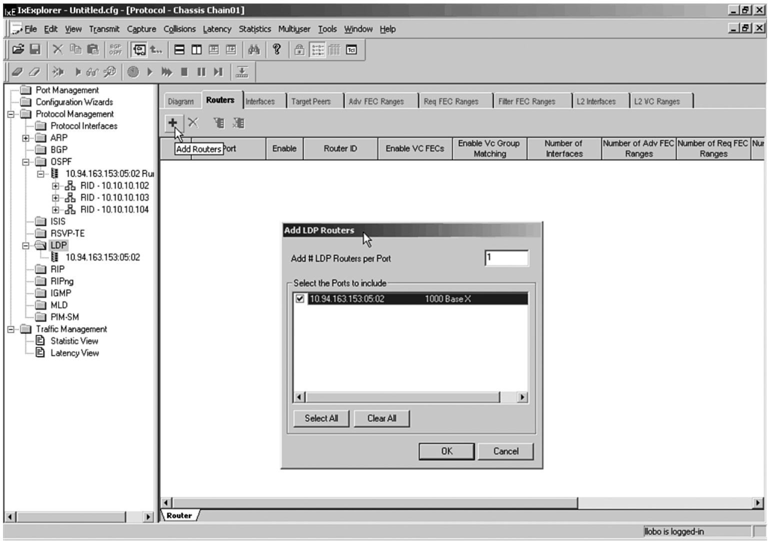
Step C—Click the **Add Routers** icon, as shown in Figure 15-92.

Step D—Step C takes you to the Add LDP Routers screen, as shown in Figure 15-92. Select the port to be included in LDP.

Step E—In this step, input value **1** in the Add # LDP Routers per Port box. This step creates the emulated LDP P router.

Step F—Click **OK** to close box.

Figure 15-92 *Add LDP Router*



Add LDP Routers

Add # LDP Routers per Port: 1

Select the Ports to include

☑ 10.94.163.153:05:02 1000 Base X

Select All | Clear All

OK | Cancel

Step 3 In this step, the P router interface properties are configured:

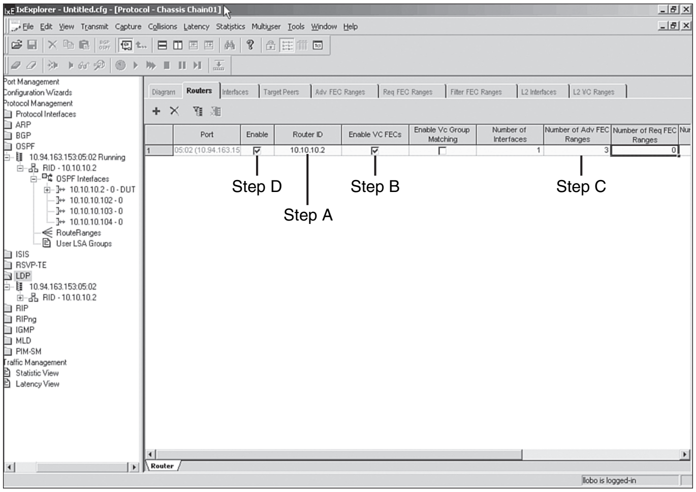
Step A—Configure the router ID to 10.10.10.2.

Step B—Ensure that **VC FECs** is checked.

Step C—Input numeric value **3** in the **Number of Adv FEC Ranges** box. This field indicates the number of FECs advertised by the P router. The P router advertises PE router interfaces 10.10.10.102 to 10.10.10.104.

Step D—Enable the LDP router by clicking the checkbox, as shown in Figure 15-93.

Figure 15-93 *Configure the LDP Interface for P Router*



IxExplorer - Untitled.cfg - [Protocol - Chassis Chain01]

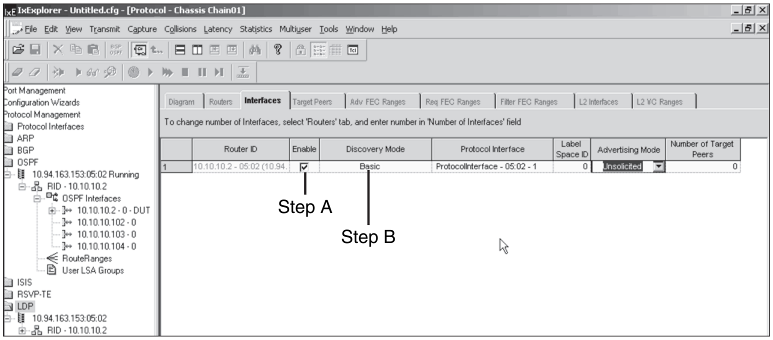
	Port	Enable	Router ID	Enable VC FECs	Enable Vc Group Matching	Number of Interfaces	Number of Adv FEC Ranges	Number of Req FEC Ranges
1	05:02 (10.94.163.15	☑	10.10.10.2	☑	☐	1	3	0

Step 4 In this step, the LDP parameters for the P router are defined by clicking on the **Interfaces** tab, as shown in Figure 15-94:

Step A—Select the Protocol Interface 5:02-1, which is 10.10.10.102. Select the **Basic LDP Discovery Mode**.

Step B—Enable the LDP router interface.

Figure 15-94 *Configure the LDP Interface for P Router*



IxExplorer - Untitled.cfg - [Protocol - Chassis Chain01]

To change number of Interfaces, select 'Routers' tab, and enter number in 'Number of Interfaces' field

	Router ID	Enable	Discovery Mode	Protocol Interface	Label Space ID	Advertising Mode	Number of Target Peers
1	10.10.10.2 - 05:02 (10.94.	☑	Basic	ProtocolInterface - 05:02 - 1	0	Unsolicited	0

Step 5 In this step, the LDP parameters (networks and labels) for the P router are defined. Click the **Adv FEC Ranges** tab:

Step A—Configure networks as shown in Figure 15-95.

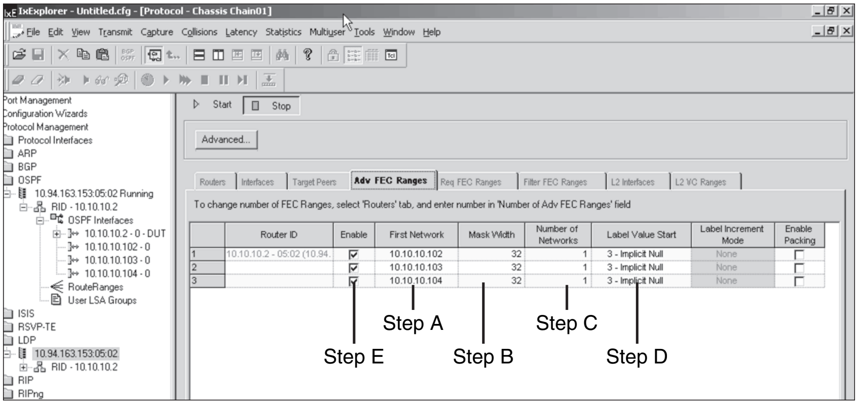
Step B—Configure the network masks.

Step C—Ensure that number of networks is "1."

Step D—Configure the label start value to implicit null.

Step E—Enable all the FECs.

Figure 15-95 *Configure the FEC to Be Advertised*

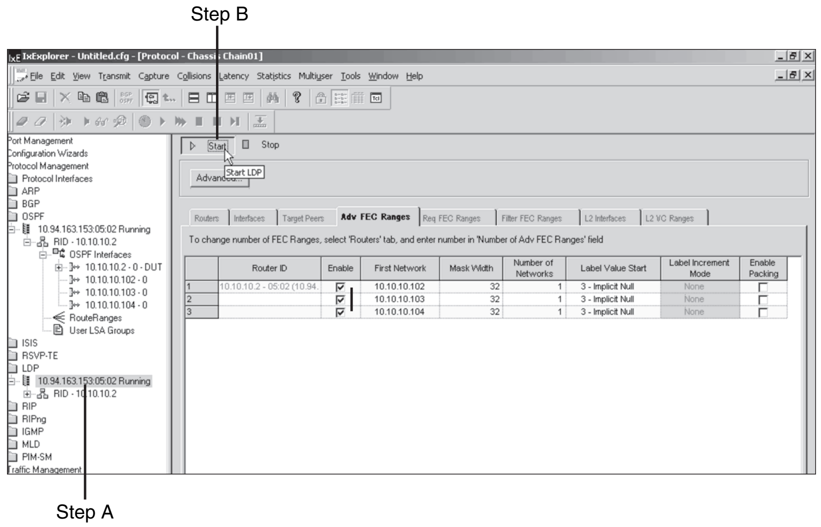


To change number of FEC Ranges, select 'Routers' tab, and enter number in 'Number of Adv FEC Ranges' field

	Router ID	Enable	First Network	Mask Width	Number of Networks	Label Value Start	Label Increment Mode	Enable Packing
1	10.10.10.2 - 05:02 (10.94.	☑	10.10.10.102	32	1	3 - Implicit Null	None	☐
2		☑	10.10.10.103	32	1	3 - Implicit Null	None	☐
3		☑	10.10.10.104	32	1	3 - Implicit Null	None	☐

Step 6 Finally, start the LDP session, as shown in Figure 15-96. Follow the steps shown in Figure 15-96.

Figure 15-96 *Start LDP*



To change number of FEC Ranges, select 'Routers' tab, and enter number in 'Number of Adv FEC Ranges' field

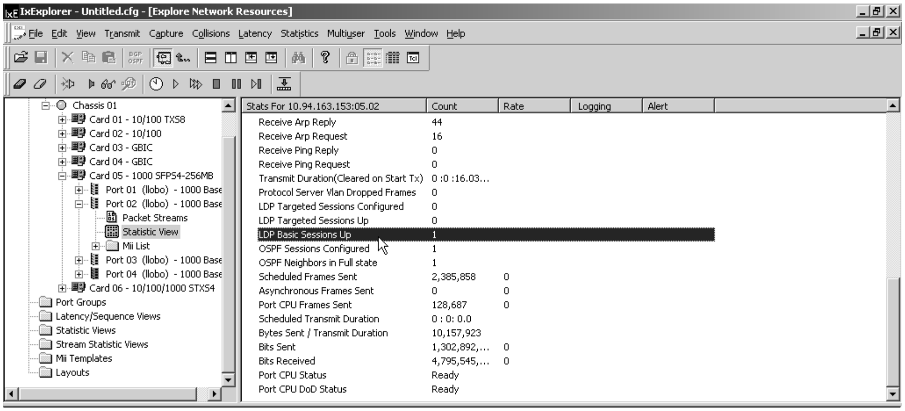
	Router ID	Enable	First Network	Mask Width	Number of Networks	Label Value Start	Label Increment Mode	Enable Packing
1	10.10.10.2 - 05:02 (10.94.	☑	10.10.10.102	32	1	3 - Implicit Null	None	☐
2		☑	10.10.10.103	32	1	3 - Implicit Null	None	☐
3		☑	10.10.10.104	32	1	3 - Implicit Null	None	☐

Step 7 To verify the LDP session,

Step A—Go to **Explore Network Resources**, as shown in Figure 15-97.

Step B—Go to the Statistic View for Port 5:02 and scroll down the right pane to view the LDP Basic Session. In this case, the P router has an LDP session with PE1, which is the DUT. Example 15-12 displays the **show mpls ldp neighbor 10.10.10.2** output.

Figure 15-97 *Verify LDP on IXIA*


IxExplorer - Untitled.cfg - [Explore Network Resources]
File Edit View Transmit Capture Collisions Latency Statistics Multiuser Tools Window Help
BGP OSPF
Tcl
Chassis 01
Card 01 - 10/100 TXS8
Card 02 - 10/100
Card 03 - GBIC
Card 04 - GBIC
Card 05 - 1000 SFPS4-256MB
Port 01 (llobo) - 1000 Base
Port 02 (llobo) - 1000 Base
Packet Streams
Statistic View
Mii List
Port 03 (llobo) - 1000 Base
Port 04 (llobo) - 1000 Base
Card 06 - 10/100/1000 STXS4
Port Groups
Latency/Sequence Views
Statistic Views
Stream Statistic Views
Mii Templates
Layouts

Stats For 10.94.163.153:05.02	Count	Rate	Logging	Alert
Receive Arp Reply	44			
Receive Arp Request	16			
Receive Ping Reply	0			
Receive Ping Request	0			
Transmit Duration(Cleared on Start Tx)	0 :0 :16.03...			
Protocol Server Vlan Dropped Frames	0			
LDP Targeted Sessions Configured	0			
LDP Targeted Sessions Up	0			
LDP Basic Sessions Up	1			
OSPF Sessions Configured	1			
OSPF Neighbors in Full state	1			
Scheduled Frames Sent	2,385,858	0		
Asynchronous Frames Sent	0	0		
Port CPU Frames Sent	128,687	0		
Scheduled Transmit Duration	0 : 0: 0.0			
Bytes Sent / Transmit Duration	10,157,923			
Bits Sent	1,302,892,...	0		
Bits Received	4,795,545,...	0		
Port CPU Status	Ready			
Port CPU DoD Status	Ready			

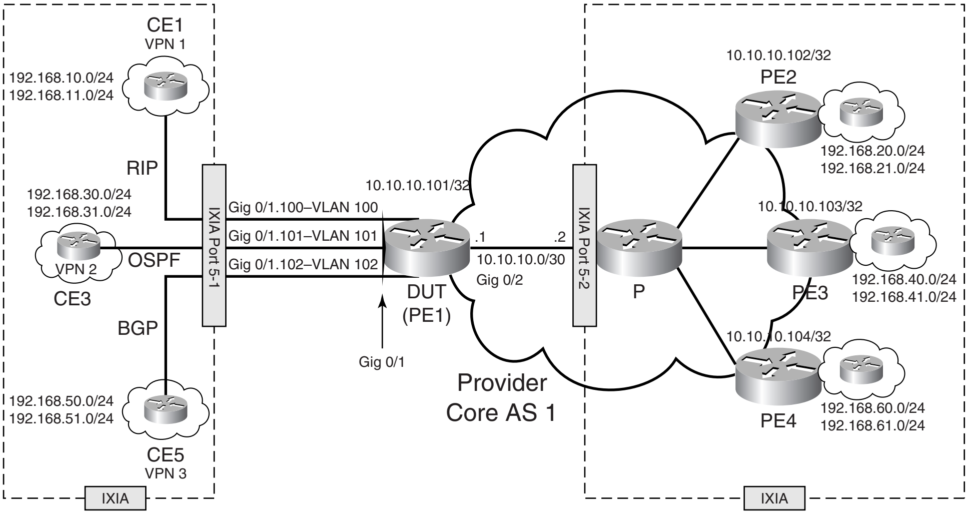
Example 15-12 **show mpls ldp neighbor 10.10.10.2** *on DUT*

```
DUT#show mpls ldp neighbor 10.10.10.2
    Peer LDP Ident: 10.10.10.2:0; Local LDP Ident 10.10.10.101:0
        TCP connection: 10.10.10.2.646 - 10.10.10.101.20824
        State: Oper; Msgs sent/rcvd: 6130/5363; Downstream
        Up time: 14:53:44
        LDP discovery sources:
          GigabitEthernet0/2, Src IP addr: 10.10.10.2
        Addresses bound to peer LDP Ident:
          10.10.10.2
```

Testing L3 MPLS VPN with IXIA

Figure 15-98 shows an L3 MPLS VPN network. Multiple 802.1Q sub-interfaces are configured on the CE interface GIG0/1 on the DUT. These interfaces are VRF-enabled and connect to Card 5, Port 1 on the IXIA. Port Gig0/2 on the DUT is connected to Card 5, Port 2 on the IXIA. Port 5-2 on IXIA simulates the provider network comprising the P router and PE Routers PE2, PE3, and PE4. These routers have individual MP-iBGP sessions with the DUT (PE1) and advertise VPNv4 routes to the DUT.

Figure 15-98 *MPLS VPN Network*



The following sections demonstrate the following:

- Configuring MP-iBGP on the IXIA
- PE-CE routing
- Traffic generation

It is imperative that the MPLS is enabled on the IXIA prior to configuring the following. Refer to the section “Basic MPLS Configuration Procedure on IXIA” in this chapter prior to implementing the steps in following sections.

Configuring MP-iBGP on IXIA

The following outlines the steps for the configuration of MP-iBGP between the IXIA and the DUT ports:

Step 1 In the Protocol window, perform the following steps:

Step A—Click **Port 5-2** in the BGP folder.

Step B—Go to the Peers tab.

Step C—Add BGP neighbors by clicking three times on the **Add Neighbor** icon.

Step D—Change the local IP for each of the interfaces to 10.10.10.102, 10.10.10.103, and 10.10.10.104, respectively. These symbolize the loopback interfaces on PE2, PE3, and PE4.

Step E—Change the number of neighbors for each to “1.”

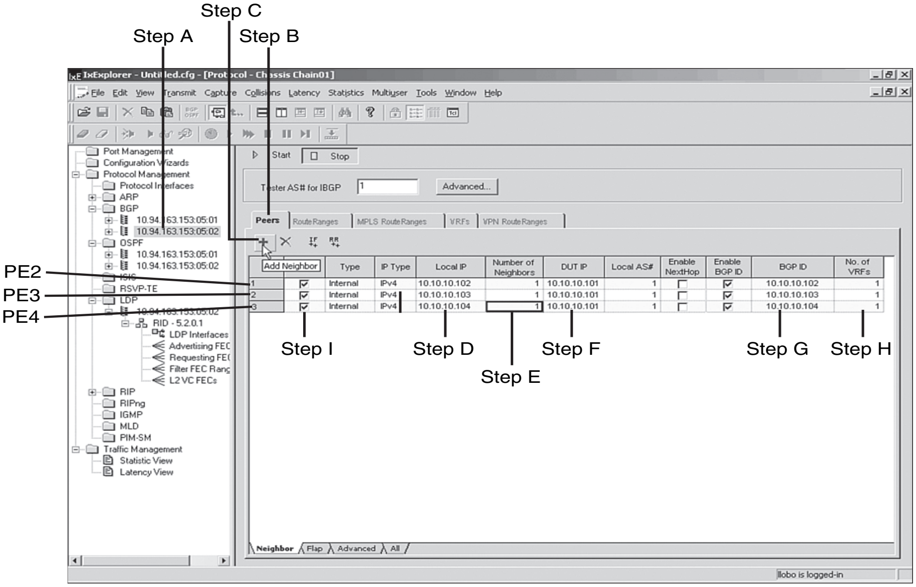
Step F—Change the DUT IP to 10.10.10.101. This is the loopback on the DUT.

Step G—Change the BGP ID, as shown in Figure 15-99.

Step H—Each peer in this case has a single VRF. Change the value to 1 for each neighbor.

Step I—Enable all the BGP neighbors.

Figure 15-99 *Configure BGP Peers*



Tester AS# for IBGP: 1

		Type	IP Type	Local IP	Number of Neighbors	DUT IP	Local AS#	Enable NextHop	Enable BGP ID	BGP ID	No. of VRFs
1	☑	Internal	IPv4	10.10.10.102	1	10.10.10.101	1	☐	☑	10.10.10.102	1
2	☑	Internal	IPv4	10.10.10.103	1	10.10.10.101	1	☐	☑	10.10.10.103	1
3	☑	Internal	IPv4	10.10.10.104	1	10.10.10.101	1	☐	☑	10.10.10.104	1

Step 2 In this step, the attributes for the VRFs are configured as shown in the following steps:

Step A—Click the **VRFs** tab.

Step B—Configure Admin part AS Number to 1 for all peers. This signifies the AS portion export route target (RT) value "AS:nn."

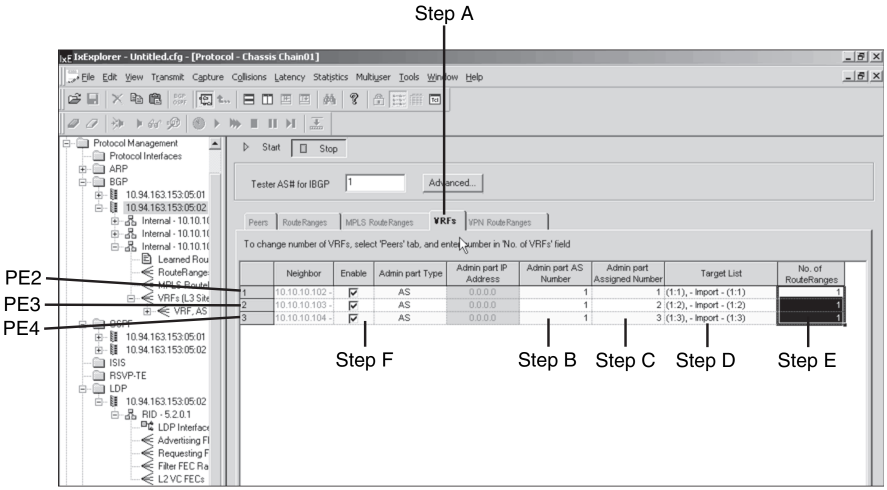
Step C—Configure the Admin part Assigned Number to the value, as shown in Figure 15-100.

Step D—Configure the RT value in such a way that it matches the export RT configured in the DUT. For example, the DUT is configured to export RIP routes with RT 1:1. Therefore, VRF on peer 10.10.10.102 is configured to import RIP routes with RT value 1:1.

Step E—Change the number of route ranges for each peer to 1, which maps to the networks to be advertised.

Step F—Enable the VRF.

Figure 15-100 *Configure L3 VRFs*


Step A
IxExplorer - Untitled.cfg - [Protocol - Chassis Chain01]
File Edit View Transmit Capture Collisions Latency Statistics Multiuser Tools Window Help
Start
Stop
Peers
RouteRanges
MPLS RouteRanges
VRFs
VPN RouteRanges
PE2
PE3
PE4
Step F
Step B
Step C
Step D
Step E

Tester AS# for IBGP: 1

To change number of VRFs, select 'Peers' tab, and enter number in 'No. of VRFs' field

	Neighbor	Enable	Admin part Type	Admin part IP Address	Admin part AS Number	Admin part Assigned Number	Target List	No. of RouteRanges
1	10.10.10.102 -	☑	AS	0.0.0.0	1	1	(1:1), - Import - (1:1)	1
2	10.10.10.103 -	☑	AS	0.0.0.0	1	2	(1:2), - Import - (1:2)	1
3	10.10.10.104 -	☑	AS	0.0.0.0	1	3	(1:3), - Import - (1:3)	1

Step 3 In this step, the VPNv4 routes are configured that will be advertised by each remote peer to the DUT:

Step A—Click **VPN Route Ranges**, as shown in Figure 15-101.

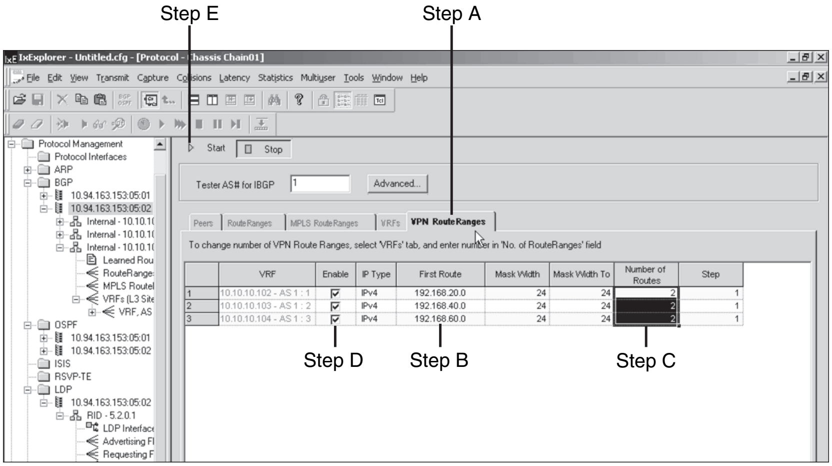
Step B—Change the routes as shown in Figure 15-101. PE2 will advertise networks starting with 192.168.20.0.

Step C—Change the number of routes to 2. This means PE2 advertises networks 192.168.20.0 and 192.168.21.0.

Step D—Enable the route ranges for each peer.

Step E—Start BGP routing by clicking the **Start** icon.

Figure 15-101 *Configure VPNv4 Route Ranges*


Step E
Step A
IxExplorer - Untitled.cfg - [Protocol - Chassis Chain01]
File Edit View Transmit Capture Collisions Latency Statistics Multiuser Tools Window Help
Start
Stop
Peers
RouteRanges
MPLS RouteRanges
VRFs
VPN RouteRanges
Step D
Step B
Step C

Tester AS# for IBGP: 1

To change number of VPN Route Ranges, select 'VRFs' tab, and enter number in 'No. of RouteRanges' field

	VRF	Enable	IP Type	First Route	Mask Width	Mask Width To	Number of Routes	Step
1	10.10.10.102 - AS 1 : 1	☑	IPv4	192.168.20.0	24	24	2	1
2	10.10.10.103 - AS 1 : 2	☑	IPv4	192.168.40.0	24	24	2	1
3	10.10.10.104 - AS 1 : 3	☑	IPv4	192.168.60.0	24	24	2	1

Verify MP-iBGP Connectivity Between IXIA and DUT

The following steps outline the verification of MP-iBGP connectivity between the IXIA and the DUT:

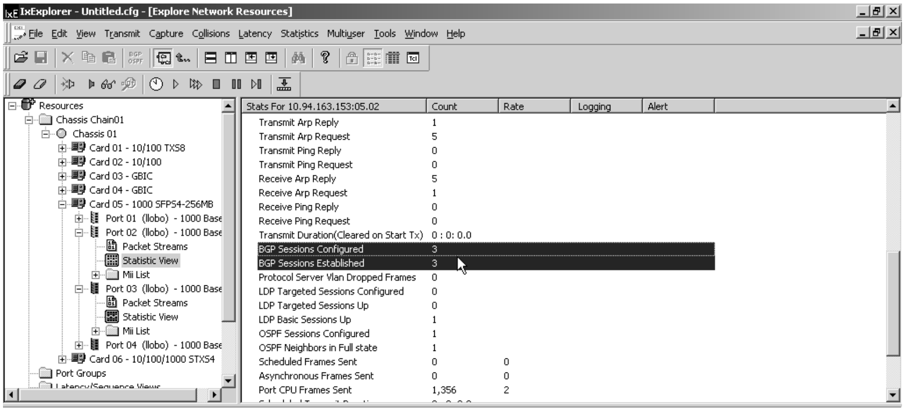
Step 1 On the DUT, verify by issuing **show ip bgp vpnv4 all summary**. Example 15-13 shows the output of **show ip bgp vpnv4 all summary** on the DUT. As seen in the output, the DUT has formed an MP-iBGP session with all simulated PEs on the IXIA.

Example 15-13 show ip bgp vpnv4 all summary

```
DUT#show ip bgp vpnv4 all summary | begin 10.10.10.102
10.10.10.102    4     1    1864    1918      463    0    0 00:00:18        2
10.10.10.103    4     1     431     491      463    0    0 00:00:17        2
10.10.10.104    4     1     429     489      463    0    0 00:00:19        2
```

Step 2 On the IXIA, verify the MP-iBGP connectivity by going to the Explore Network Resources window and clicking **Statistic View**, as shown in Figure 15-102.

Figure 15-102 *LDP Verification on IXIA*


IxExplorer - Untitled.cfg - [Explore Network Resources]
File Edit View Transmit Capture Collisions Latency Statistics Multiuser Tools Window Help
Resources
Chassis Chain01
Chassis 01
Card 01 - 10/100 TXS8
Card 02 - 10/100
Card 03 - GBIC
Card 04 - GBIC
Card 05 - 1000 SFPS4-256MB
Port 01 (llobo) - 1000 Base
Port 02 (llobo) - 1000 Base
Packet Streams
Statistic View
Mii List
Port 03 (llobo) - 1000 Base
Packet Streams
Statistic View
Mii List
Port 04 (llobo) - 1000 Base
Card 06 - 10/100/1000 STXS4
Port Groups

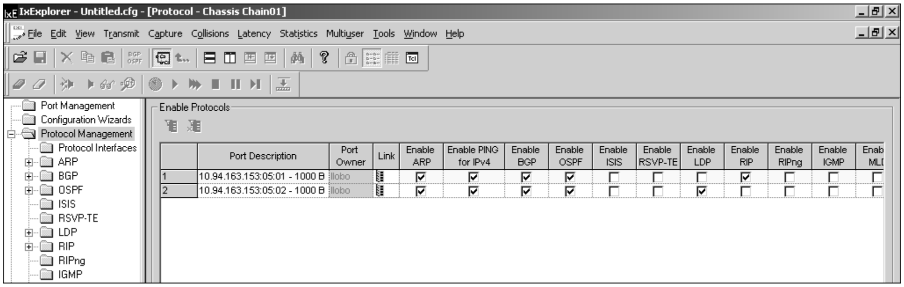
Stats For 10.94.163.153:05.02	Count	Rate	Logging	Alert
Transmit Arp Reply	1			
Transmit Arp Request	5			
Transmit Ping Reply	0			
Transmit Ping Request	0			
Receive Arp Reply	5			
Receive Arp Request	1			
Receive Ping Reply	0			
Receive Ping Request	0			
Transmit Duration(Cleared on Start Tx)	0 : 0: 0.0			
BGP Sessions Configured	3			
BGP Sessions Established	3			
Protocol Server Vlan Dropped Frames	0			
LDP Targeted Sessions Configured	0			
LDP Targeted Sessions Up	0			
LDP Basic Sessions Up	1			
OSPF Sessions Configured	1			
OSPF Neighbors in Full state	1			
Scheduled Frames Sent	0	0		
Asynchronous Frames Sent	0	0		
Port CPU Frames Sent	1,356	2		

PE-CE Configuration on the IXIA

In this section, RIP PE-CE routing, BGP PE-CE routing, and OSPF PE-CE routing are configured on the IXIA. Ensure that the following steps are performed prior to configuring PE-CE routing:

Step 1 Prior to configuring, ensure that protocols RIP, BGP, and OSPF are enabled on Port 5-1, as shown in Figure 15-103.

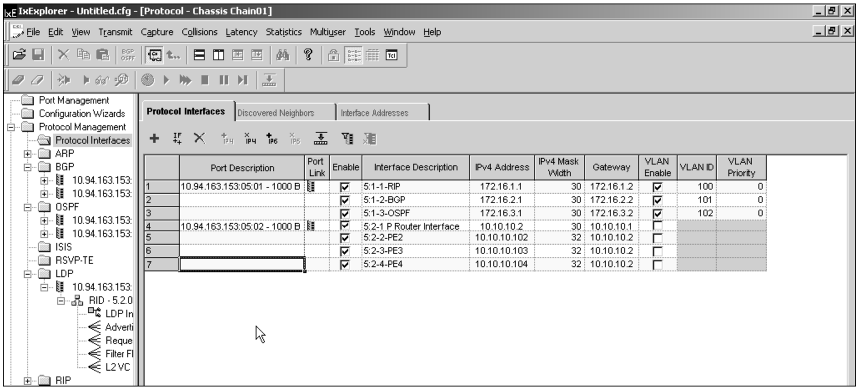
Figure 15-103 *Enabling Protocols*



	Port Description	Port Owner	Link	Enable ARP	Enable PING for IPv4	Enable BGP	Enable OSPF	Enable ISIS	Enable RSVP-TE	Enable LDP	Enable RIP	Enable RIPng	Enable IGMP	Enab MLI
1	10.94.163.153:05:01 - 1000 B	llobo		☑	☑	☑	☑	☐	☐	☐	☑	☐	☐	☐
2	10.94.163.153:05:02 - 1000 B	llobo		☑	☑	☑	☑	☐	☐	☑	☐	☐	☐	☐

Step 2 Go to the Protocol window and ensure that Protocol Interfaces shows the relevant interfaces on Port 5-1, as shown in Figure 15-104.

Figure 15-104 *Configure CE Interfaces on IXIA Port 5-1*



	Port Description	Port Link	Enable	Interface Description	IPv4 Address	IPv4 Mask Width	Gateway	VLAN Enable	VLAN ID	VLAN Priority
1	10.94.163.153:05:01 - 1000 B		☑	5:1-1-RIP	172.16.1.1	30	172.16.1.2	☑	100	0
2			☑	5:1-2-BGP	172.16.2.1	30	172.16.2.2	☑	101	0
3			☑	5:1-3-OSPF	172.16.3.1	30	172.16.3.2	☑	102	0
4	10.94.163.153:05:02 - 1000 B		☑	5:2-1 P Router Interface	10.10.10.2	30	10.10.10.1	☐		
5			☑	5:2-2-PE2	10.10.10.102	32	10.10.10.2	☐		
6			☑	5:2-3-PE3	10.10.10.103	32	10.10.10.2	☐		
7			☑	5:2-4-PE4	10.10.10.104	32	10.10.10.2	☐		

RIP PE-CE Routing Configuration on the IXIA

The steps to configure RIP PE-CE routing are as follows:

Step 1 In this step, the RIP router is defined. The steps are as follows:

Step A—Click **Port 5-1** under the RIP folder, as shown in Figure 15-105.

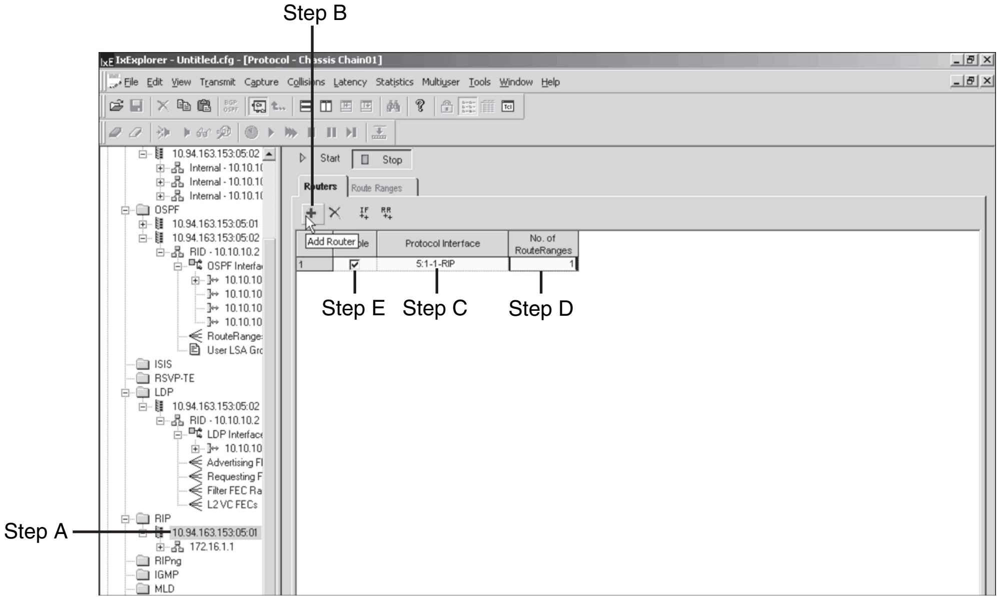
Step B—Add the RIP router by clicking on the **Add Router** icon.

Step C—Define the protocol interface, in this case 5-1:1-RIP.

Step D—Define the number of route ranges to 1.

Step E—Enable the RIP router.

Figure 15-105 *Configuring RIP Router*



Step 2 In this step, the VPNv4 routes that will be advertised by each remote peer to the DUT are configured:

Step A—Click **Route Ranges**, as shown in Figure 15-106.

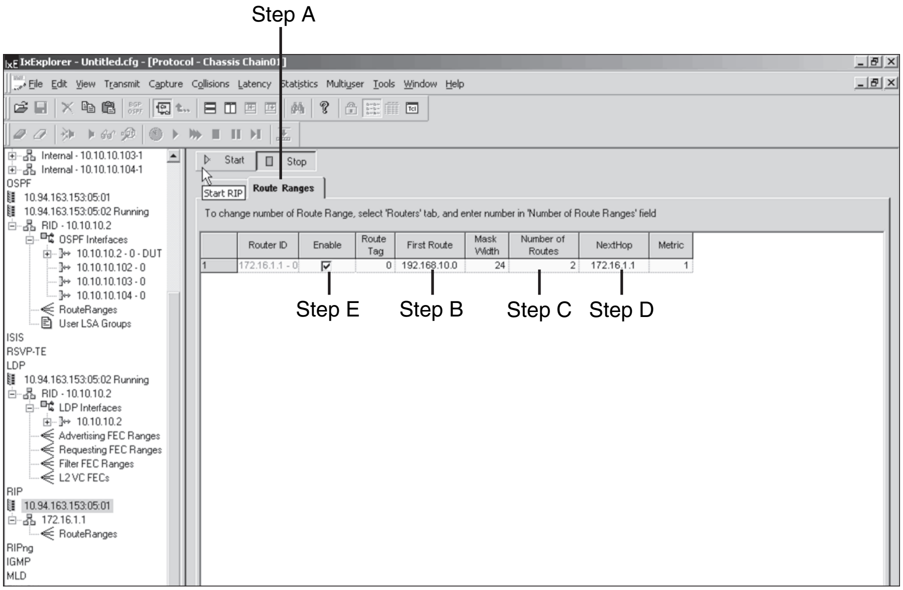
Step B—Change the routes as shown in Figure 15-106. 172.16.1.1 advertises networks starting with 192.168.10.0.

Step C—Change the number of routes to 2. This means RIP interface 172.16.1.1 advertises networks 192.168.10.0 and 192.168.11.0.

Step D—Ensure that the next hop advertised in the update is 172.16.1.1.

Step E—Enable the route range and then start RIP PE-CE routing by clicking the **Start** icon.

Figure 15-106 *Configure RIP Routes to Be Advertised by CE1*



To change number of Route Range, select 'Routers' tab, and enter number in 'Number of Route Ranges' field

	Router ID	Enable	Route Tag	First Route	Mask Width	Number of Routes	NextHop	Metric
1	172.16.1.1 - 0	☑	0	192.168.10.0	24	2	172.16.1.1	1

Verify RIP PE-CE Routing Configuration on the IXIA

The steps to verify RIP PE-CE routing are

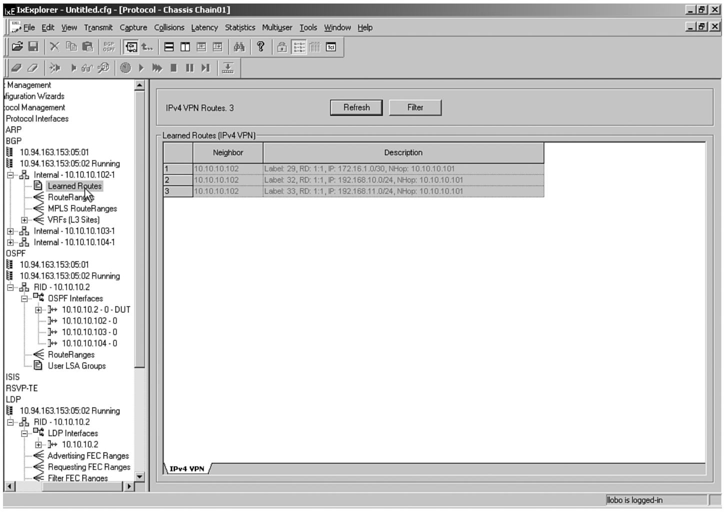
Step 1 On the DUT, verify by issuing **show ip route vrf VRF-RIP**. Example 15-14 shows the output of **show ip route vrf VRF-RIP** on the DUT.

Example 15-14 **show ip route vrf VRF-RIP**

```
DUT#show ip route vrf VRF-RIP rip
R    192.168.10.0/24 [120/1] via 172.16.1.1, 00:00:03, GigabitEthernet0/1.100
R    192.168.11.0/24 [120/1] via 172.16.1.1, 00:00:03, GigabitEthernet0/1.100
```

Step 2 On the IXIA, in the Protocol window, click the **PE2** on Port 5-2 under the BGP folder. Click **Learned Routes**. Click the **Refresh** filter to see the routes from CE1, as shown in Figure 15-107.

Figure 15-107 *View RIP Routes from CE1 on PE2—10.10.10.102*



IPv4 VPN Routes. 3

Learned Routes (IPv4 VPN)

	Neighbor	Description
1	10.10.10.102	Label: 29, RD: 1:1, IP: 172.16.1.0/30, NHop: 10.10.10.101
2	10.10.10.102	Label: 32, RD: 1:1, IP: 192.168.10.0/24, NHop: 10.10.10.101
3	10.10.10.102	Label: 33, RD: 1:1, IP: 192.168.11.0/24, NHop: 10.10.10.101

BGP PE-CE Routing Configuration on the IXIA

The steps to configure BGP PE-CE routing are as follows:

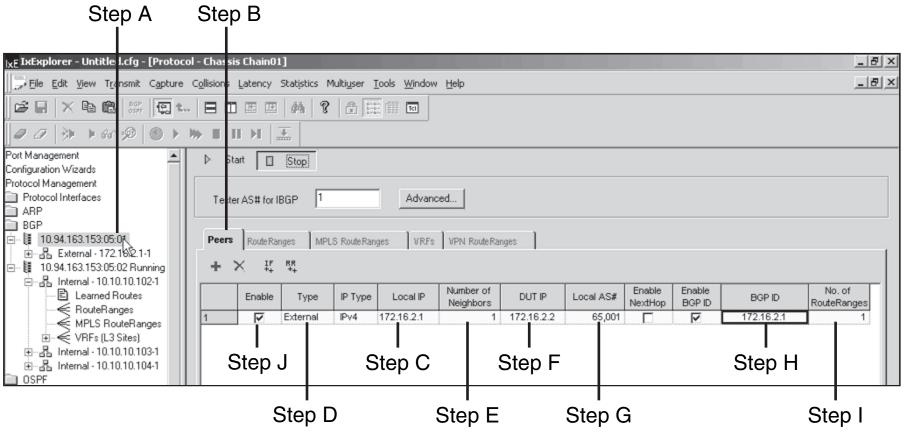
Step 1 In this step, the BGP neighbor is defined. The steps are as follows:

Step A—Click **Port 5-1** under the BGP folder, as shown in Figure 15-108.

Step B—Go to the Peers tab and click the **Add Router** (plus sign) icon.

Configure Steps C through J as shown in Figure 15-108. Note that this is an eBGP session and ensure that the CE3 AS is 65,001.

Figure 15-108 *Configure BGP Peers*



Tester AS# for IBGP: 1

	Enable	Type	IP Type	Local IP	Number of Neighbors	DUT IP	Local AS#	Enable NextHop	Enable BGP ID	BGP ID	No. of RouteRanges
1	☑	External	IPv4	172.16.2.1	1	172.16.2.2	65,001	☐	☑	172.16.2.1	1

Step 2 In this step, the route range that will be advertised by CE3 to the DUT is configured:

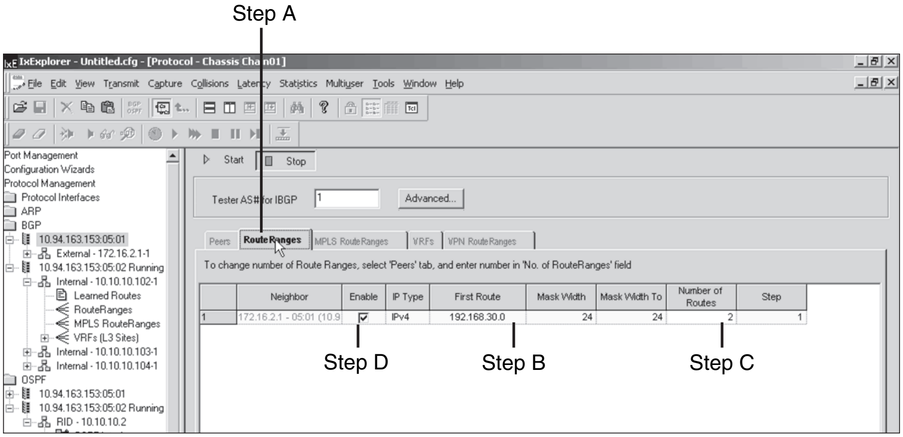
Step A—Click **Route Ranges**, as shown in Figure 15-109.

Step B—Change the routes as shown in Figure 15-109. 172.16.2.1 advertises networks starting with 192.168.30.0.

Step C—Change the number of routes to two. This means BGP peer 172.16.2.1 advertises networks 192.168.30.0 and 192.168.31.0.

Step D—Enable the route range and then start RIP PE-CE routing by clicking on the **Start** icon.

Figure 15-109 *Configure BGP Routes to Be Advertised by CE2*



Tester AS# for IBGP 1

To change number of Route Ranges, select 'Peers' tab, and enter number in 'No. of RouteRanges' field

	Neighbor	Enable	IP Type	First Route	Mask Width	Mask Width To	Number of Routes	Step
1	172.16.2.1 - 05:01 (10.9	☑	IPv4	192.168.30.0	24	24	2	1

Verify BGP PE-CE Routing Configuration

The steps to verify BGP PE-CE routing are as follows:

Step 1 On the DUT, verify by issuing **show ip bgp vpnv4 all summary**. Example 15-15 shows that the BGP neighbor relationship with 172.16.2.1 is up.

Example 15-15 **show ip bgp vpnv4 all summary**

```
DUT#show ip bgp vpnv4 all summary | begin N
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.102    4     1    2146    2208      495    0    0 02:21:03        2
10.10.10.103    4     1     713     781      495    0    0 02:21:02        2
10.10.10.104    4     1     711     779      495    0    0 02:21:04        2
172.16.2.1      4 65001     370     423      495    0    0 00:00:53        2
```

OSPF PE-CE Routing Configuration on the IXIA

The steps to configure OSPF PE-CE routing are as follows:

Step 1 In this step, the OSPF router is defined. The steps are as follows:

Step A—Click **Port 5-1** under the OSPF folder, as shown in Figure 15-110.

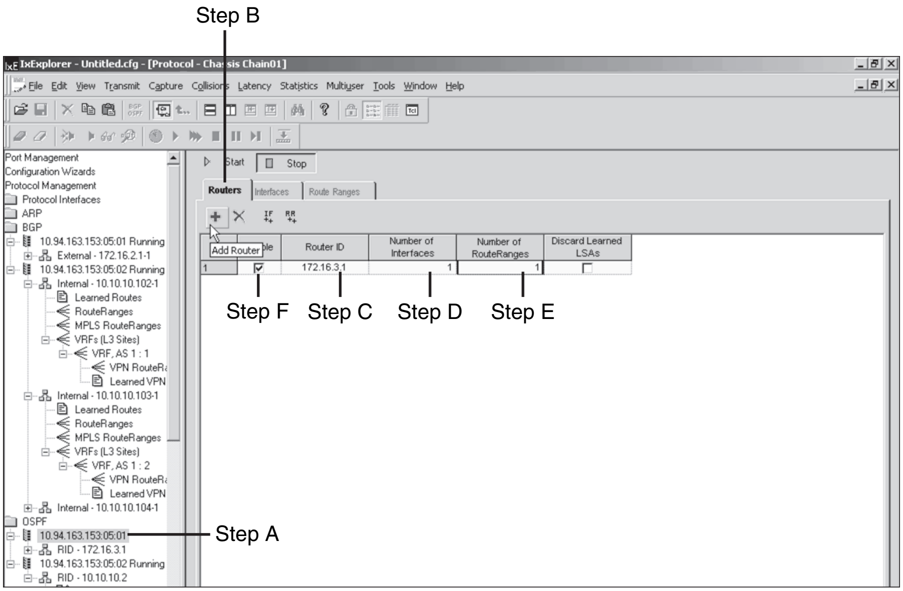
Step B—Go to the **Routers** tab and click the **Add Router** (plus sign) icon.

Step C—Configure the router ID as 172.16.3.1.

Step D—The number of interfaces is 1 because OSPF is enabled only on the 172.16.3.0 network.

Step E—Configure the number of the OSPF route range as 1.

Figure 15-110 *Configure OSPF Router*



	ble	Router ID	Number of Interfaces	Number of RouteRanges	Discard Learned LSAs
1	☑	172.16.3.1	1	1	☐

Step 2 In this step, the OSPF routers interface properties are configured:

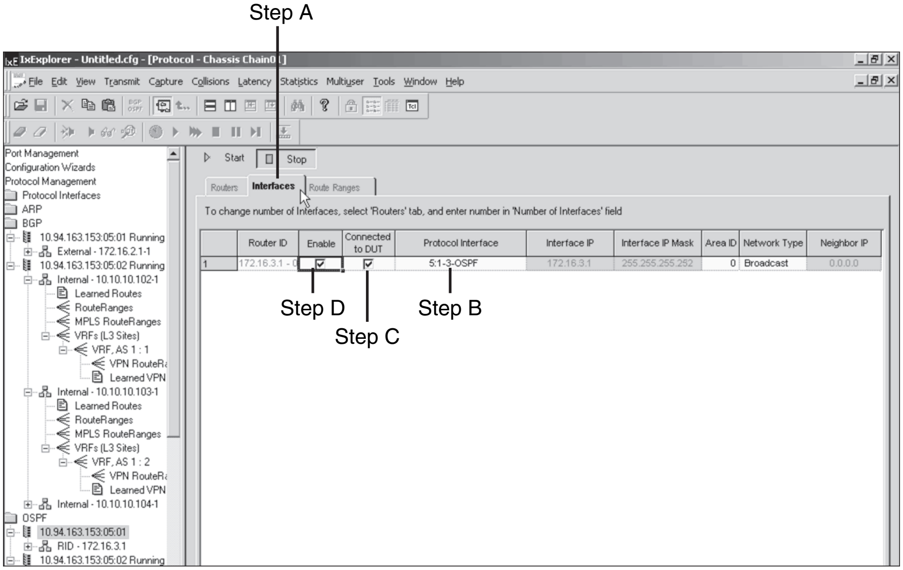
Step A—Click the **Interfaces** tab, as shown in Figure 15-111.

Step B—Select the protocol interface.

Step C—Ensure that the **Connected to DUT** check box is checked.

Step D—Enable the interface.

Figure 15-111 *Configure OSPF Interfaces*



To change number of Interfaces, select 'Routers' tab, and enter number in 'Number of Interfaces' field

	Router ID	Enable	Connected to DUT	Protocol Interface	Interface IP	Interface IP Mask	Area ID	Network Type	Neighbor IP
1	172.16.3.1 - 0	☑	☑	5:1-3-OSPF	172.16.3.1	255.255.255.252	0	Broadcast	0.0.0.0

Step 3 In this step, the route range that will be advertised by CE5 to the DUT is configured:

Step A—Click **Route Ranges**, as shown in Figure 15-112.

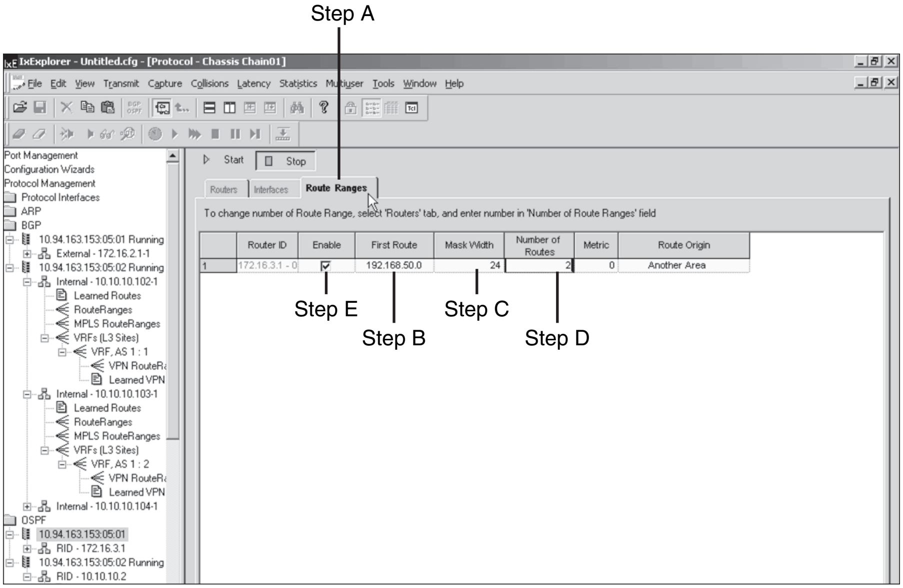
Step B—Configure the routes as shown in Figure 15-112. 172.16.3.1 advertises networks starting with 192.168.50.0.

Step C—Ensure that the mask is right; in this case, 24.

Step D—Change the number of routes to 2. This means OSPF neighbor 172.16.3.1 advertises networks 192.168.50.0 and 192.168.51.0.

Step E—Enable the route range and then start OSPF PE-CE routing by clicking the **Start** icon.

Figure 15-112 *Configure OSPF Route Range to Be Advertised by CE3*



To change number of Route Range, select 'Routers' tab, and enter number in 'Number of Route Ranges' field

	Router ID	Enable	First Route	Mask Width	Number of Routes	Metric	Route Origin
1	172.16.3.1 - 0	☑	192.168.50.0	24	2	0	Another Area

Verify OSPF PE-CE Routing Configuration

The steps to verify BGP PE-CE routing are as follows:

Step 1 On the DUT, verify by issuing **show ip ospf neighbor**. Example 15-16 shows the output of **show ip ospf neighbor** on the DUT.

Example 15-16 **show ip ospf neighbor**

```
DUT#show ip ospf neighbor | inc N|172
Neighbor ID   Pri  State          Dead Time   Address       Interface
172.16.3.1    0    FULL/DROTHER   00:00:38   172.16.3.1     GigabitEthernet0/1.102
```

Step 2 On the DUT, verify by issuing **show ip route vrf VRF-OSPF**. Example 15-17 shows the output of **show ip route vrf VRF-OSPF** on the DUT.

Example 15-17 **show ip route vrf VRF-OSPF**

```
DUT#show ip route vrf VRF-OSPF
B    192.168.61.0/24 [200/0] via 10.10.10.104, 02:53:17
B    192.168.60.0/24 [200/0] via 10.10.10.104, 02:53:17
     172.16.0.0/30 is subnetted, 1 subnets
C       172.16.3.0 is directly connected, GigabitEthernet0/1.102
O IA 192.168.51.0/24 [110/1] via 172.16.3.1, 00:01:20, GigabitEthernet0/1.102
O IA 192.168.50.0/24 [110/1] via 172.16.3.1, 00:01:20, GigabitEthernet0/1.102
```

Traffic Generation

In previous sections, you have worked with control plane generation using the IXIA. In this section, you will configure data traffic generation. You will configure data forwarding from CE1 (192.168.10.0) to CE2 (192.168.20.0) and vice versa.

CE1 to CE2

Data forwarding will take place between IXIA 5-1 to IXIA 5-2. The steps to configure data plane traffic are as follows:

Step 1 The steps are as follows:

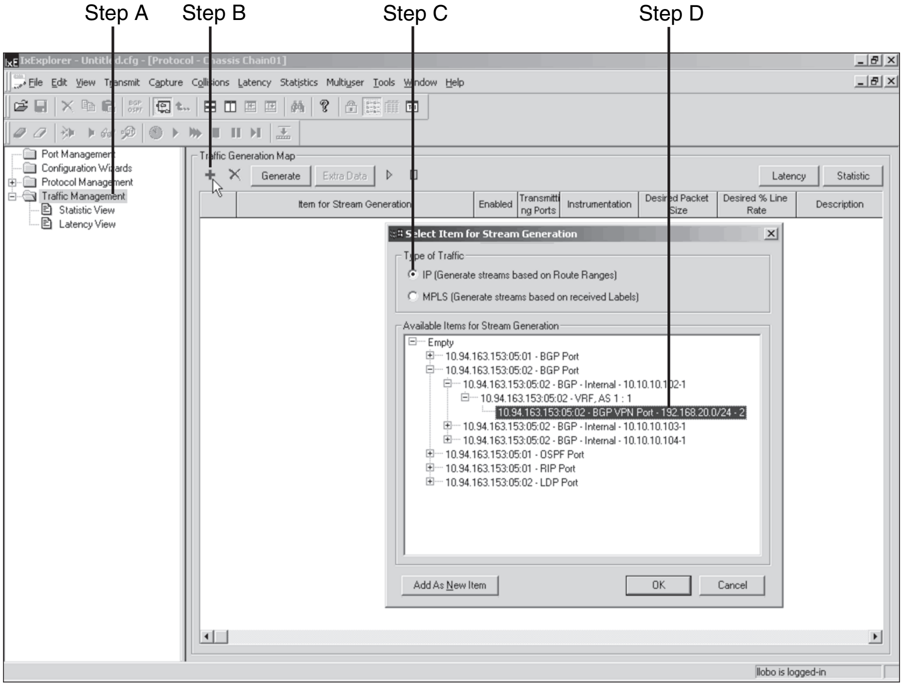
Step A—In the Protocol window, click the **Traffic Management** folder.

Step B—Click the **plus** icon, and a Select Item for Stream Generation dialog appears.

Step C—Select **IP**.

Step D—Select the destination by expanding the 5-2 BGP folder, and select the appropriate destination, as shown in Figure 15-113.

Figure 15-113 *Configure Traffic Stream from CE1 to CE2 on Port 5-1*



Select Item for Stream Generation

Type of Traffic

● IP (Generate streams based on Route Ranges)

○ MPLS (Generate streams based on received Labels)

Available Items for Stream Generation

- Empty
  - 10.94.163.153:05:01 - BGP Port
  - 10.94.163.153:05:02 - BGP Port
    - 10.94.163.153:05:02 - BGP - Internal - 10.10.10.102-1
      - 10.94.163.153:05:02 - VRF, AS 1 : 1
        - 10.94.163.153:05:02 - BGP VPN Port - 192.168.20.0/24 - 2
    - 10.94.163.153:05:02 - BGP - Internal - 10.10.10.103-1
    - 10.94.163.153:05:02 - BGP - Internal - 10.10.10.104-1
  - 10.94.163.153:05:01 - OSPF Port
  - 10.94.163.153:05:01 - RIP Port
  - 10.94.163.153:05:02 - LDP Port

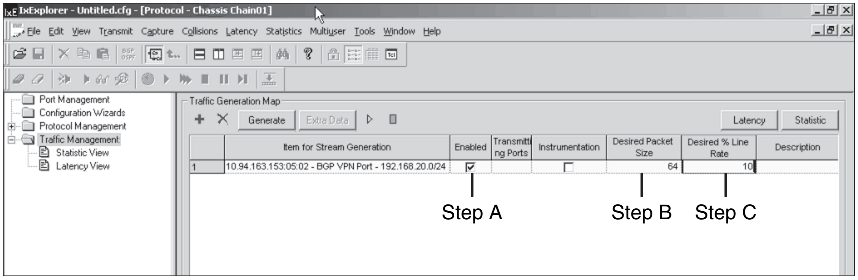
Step 2 In this step, the traffic map created previously is enabled, as shown in Figure 15-114:

Step A—Enable the traffic map.

Step B—Configure packet size to 64 bytes. This can be changed to the desired packet size if needed.

Step C—Configure the desired line rate to 10 percent, which can be varied depending on the requirement of the test.

Figure 15-114 *Configure Stream Parameters*



	Item for Stream Generation	Enabled	Transmitting Ports	Instrumentation	Desired Packet Size	Desired % Line Rate	Description
1	10.94.163.153:05:02 - BGP VPN Port - 192.168.20.0/24	☑		☐	64	10	

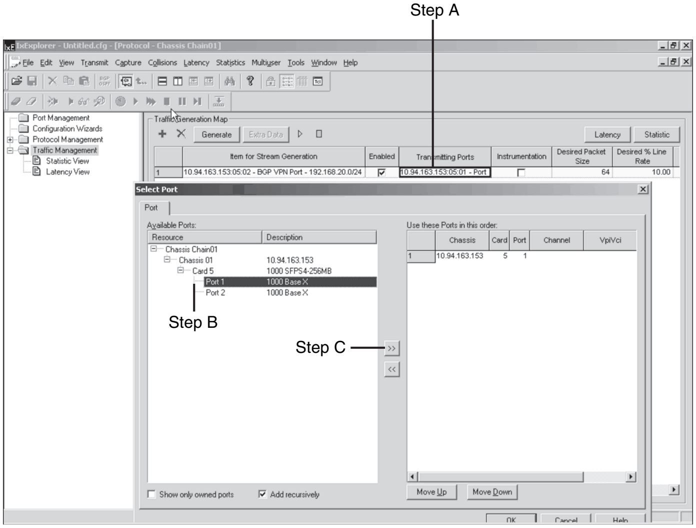
Step 3 The steps shown in Figure 15-115 are as follows:

Step A—Double-click the **Transmitting Ports** section.

Step B—Select **Port 5-1**.

Step C—Click the direction button and click **OK**.

Figure 15-115 *Define the Transmitting Port*



	Item for Stream Generation	Enabled	Transmitting Ports	Instrumentation	Desired Packet Size	Desired % Line Rate
1	10.94.163.153:05:02 - BGP VPN Port - 192.168.20.0/24	☑	10.94.163.153:05:01 - Port	☐	64	10.00

Available Ports:

Resource	Description
Chassis Chain01	
Chassis 01	10.94.163.153
Card 5	1000 SFPS4-256MB
Port 1	1000 Base X
Port 2	1000 Base X

Use these Ports in this order:

	Chassis	Card	Port	Channel	VpiVci
1	10.94.163.153	5	1		

☐ Show only owned ports ☑ Add recursively

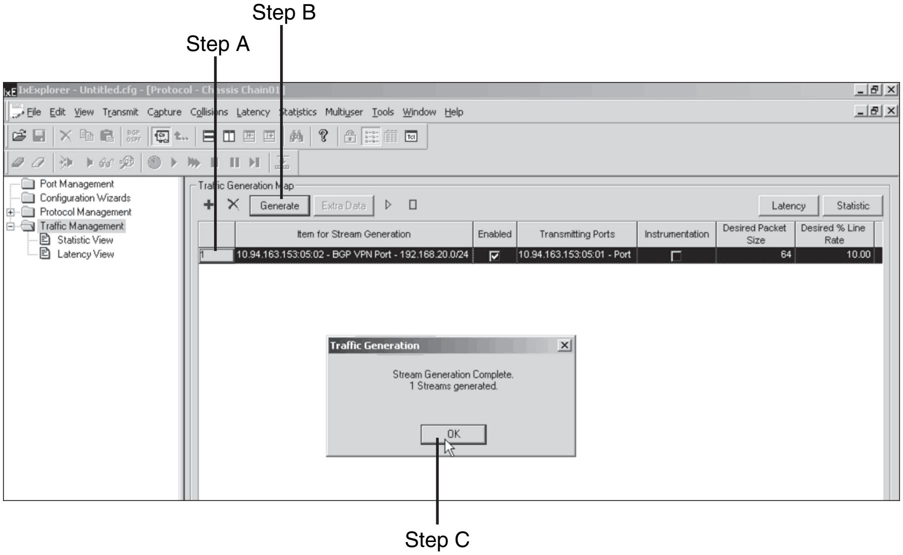
Step 4 The steps shown in Figure 15-116 are as follows:

Step A—Select the traffic map.

Step B—Click the **Generate** button.

Step C—A dialog box indicating that the stream is generated appears. Click **OK**.

Figure 15-116 *Generate the Traffic Stream*



	Item for Stream Generation	Enabled	Transmitting Ports	Instrumentation	Desired Packet Size	Desired % Line Rate
1	10.94.163.153:05:02 - BGP VPN Port - 192.168.20.0/24	☑	10.94.163.153:05:01 - Port	☐	64	10.00

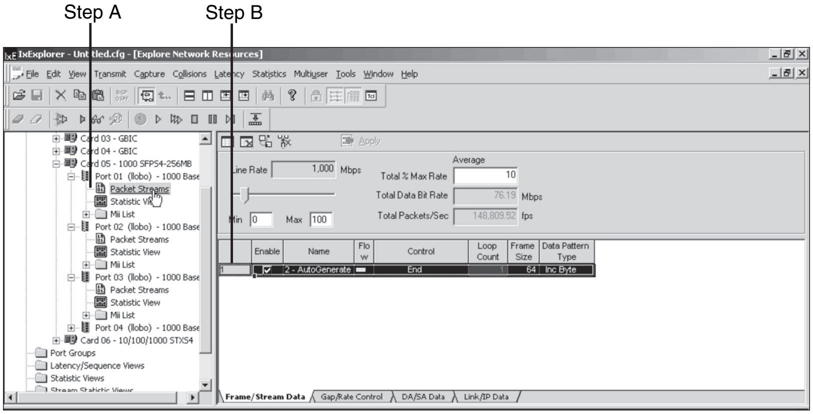
Stream Generation Complete.
1 Streams generated.

Step 5 This optional step is shown in Figure 15-117. The purpose of adding signatures to the packet is to clearly distinguish the data packet from other packets. In this step, a signature is added to the packet so that the packets can be accurately counted. Go to the Explore Network Resources window:

Step A—Select **Packet Stream** under Card 5, Port 1.

Step B—Select the stream in the right pane and double-click to go to Step 6.

Figure 15-117 *Select the Auto-Generated Stream Under Port 5-1*


Step A
Step B
IxExplorer - Untitled.cfg - [Explore Network Resources]
File Edit View Transmit Capture Collisions Latency Statistics Multiuser Tools Window Help
Apply
Card 03 - GBIC
Card 04 - GBIC
Card 05 - 1000 SFPS4-256MB
Port 01 (llobo) - 1000 Base
Packet Streams
Statistic View
Mii List
Port 02 (llobo) - 1000 Base
Packet Streams
Statistic View
Mii List
Port 03 (llobo) - 1000 Base
Packet Streams
Statistic View
Mii List
Port 04 (llobo) - 1000 Base
Card 06 - 10/100/1000 STXS4
Port Groups
Latency/Sequence Views
Statistic Views
Frame/Stream Data
Gap/Rate Control
DA/SA Data
Link/IP Data

Line Rate 1,000 Mbps
Average
Total % Max Rate 10
Total Data Bit Rate 76.19 Mbps
Total Packets/Sec 148,809.52 fps
Min 0 Max 100

	Enable	Name	Flow	Control	Loop Count	Frame Size	Data Pattern Type
1	☑	2 - AutoGenerate		End	1	64	Inc Byte

Step 6 This is an optional step. The following steps are as shown in Figure 15-118:

Step A—Select **UDF5** (User Data Field) in the Frame Data tab.

Step B—Configure the offset to 50.

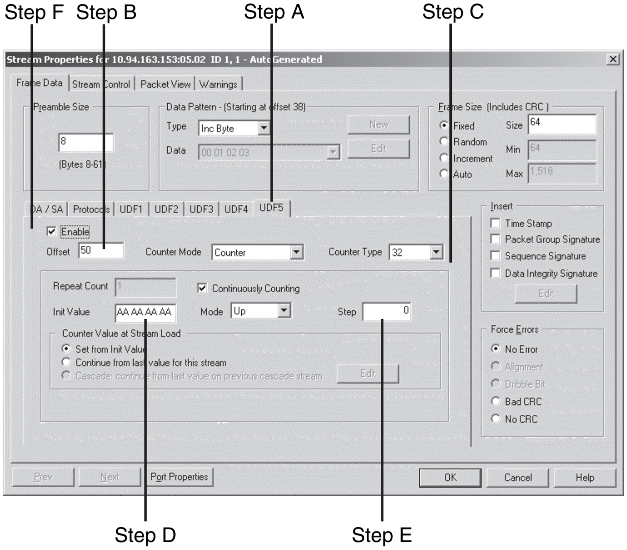
Step C—Select the counter type as 32.

Step D—Configure the 32-bit pattern "AA AA AA AA." This is your signature in the packet.

Step E—Select step size as 0.

Step F—Enable the UDF.

Figure 15-118 *Configure Packet Signature*



Preamble Size 8 (Bytes 8-61)
Data Pattern - (Starting at offset 38)
Type Inc Byte
Data 00 01 02 03
Frame Size (Includes CRC)
● Fixed Size 64
○ Random Min 64
○ Increment Max 1,518
○ Auto
☑ Enable
Offset 50 Counter Mode Counter Counter Type 32
Repeat Count 1 ☑ Continuously Counting
Init Value AA AA AA AA Mode Up Step 0
Counter Value at Stream Load
● Set from Init Value
○ Continue from last value for this stream
○ Cascade: continue from last value on previous cascade stream
Insert
☐ Time Stamp
☐ Packet Group Signature
☐ Sequence Signature
☐ Data Integrity Signature
Force Errors
● No Error
○ Alignment
○ Dribble Bit
○ Bad CRC
○ No CRC

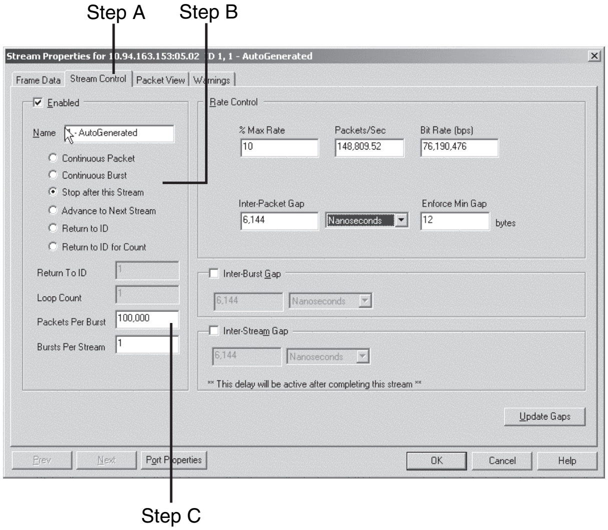
Step 7 This is an optional step. In this step, properties of the stream are configured as shown in Figure 15-119. This stream will be configured for a definite packet count:

Step A—Select the **Stream Control** tab.

Step B—Select **Stop after this Stream** so that a definite amount of packets can be sent.

Step C—Configure the number of packets to be 100,000.

Figure 15-119 *Define Stream Properties*



☑ Enabled

Name: - AutoGenerated

○ Continuous Packet
○ Continuous Burst
● Stop after this Stream
○ Advance to Next Stream
○ Return to ID
○ Return to ID for Count

Return To ID: 1
Loop Count: 1
Packets Per Burst: 100,000
Bursts Per Stream: 1

% Max Rate: 10
Packets/Sec: 148,809.52
Bit Rate (bps): 76,190,476
Inter-Packet Gap: 6,144 Nanoseconds
Enforce Min Gap: 12 bytes

☐ Inter-Burst Gap: 6,144 Nanoseconds

☐ Inter-Stream Gap: 6,144 Nanoseconds

** This delay will be active after completing this stream **

Step 8 In Steps 6 and 7, the signature in the packet stream originating from Port 5-1 was introduced. In this step, Port 5-2 is configured so that it can receive the correct packet with the signatures introduced earlier, as shown in Figure 15-120:

Step A—Select **Card 5**, **Port 2**.

Step B—Double-click **Filter, Statistics, Receive Mode**.

Step C—Select **User Defined Statistic 1**.

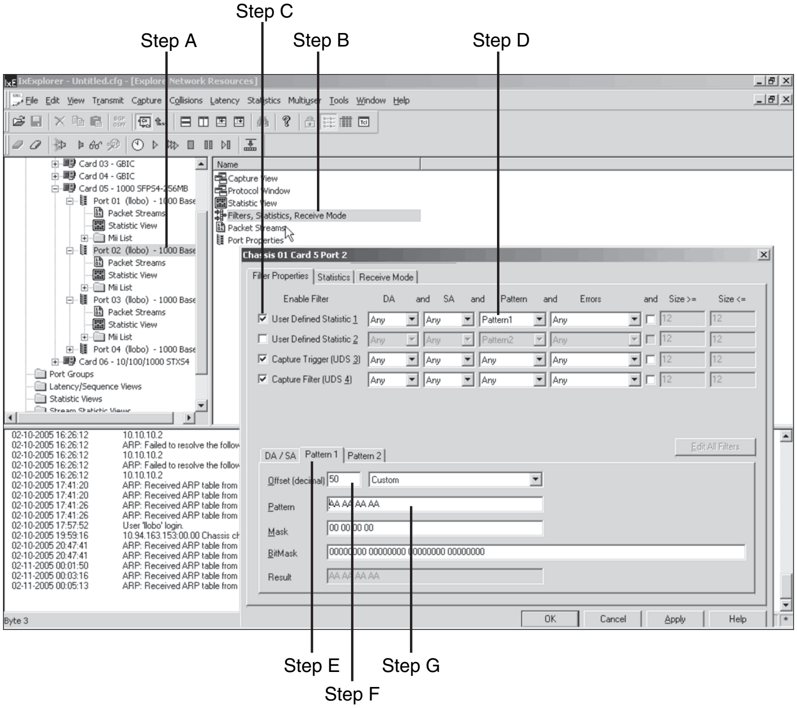
Step D—Select **Pattern1**.

Step E—Select **Pattern 1** tab.

Step F—Configure the offset as 50. This should be the same as configured in Step 6.

Step G—Configure the pattern. The pattern should match the pattern configured in Step 7.

Figure 15-120 *Configure the Receive Port 5-2*



Enable Filter	DA	and SA	and Pattern	and Errors	and	Size >=	Size <=
☑ User Defined Statistic 1	Any	Any	Pattern1	Any	☐	12	12
☐ User Defined Statistic 2	Any	Any	Pattern2	Any	☐	12	12
☑ Capture Trigger (UDS 3)	Any	Any	Any	Any	☐	12	12
☑ Capture Filter (UDS 4)	Any	Any	Any	Any	☐	12	12

Offset (decimal) 50 Custom

Pattern AA AA AA AA

Mask 00 00 00 00

BitMask 00000000 00000000 00000000 00000000

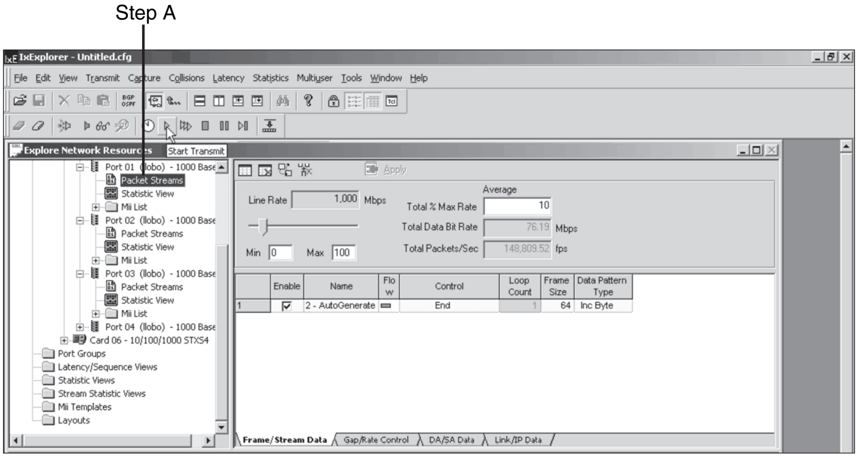
Result AA AA AA AA

```
02-10-2005 16:26:12    10.10.10.2
02-10-2005 16:26:12    ARP: Failed to resolve the follow
02-10-2005 16:26:12    10.10.10.2
02-10-2005 16:26:12    ARP: Failed to resolve the follow
02-10-2005 16:26:12    10.10.10.2
02-10-2005 17:41:20    ARP: Received ARP table from
02-10-2005 17:41:20    ARP: Received ARP table from
02-10-2005 17:41:26    ARP: Received ARP table from
02-10-2005 17:41:26    ARP: Received ARP table from
02-10-2005 17:57:52    User 'llobo' login.
02-10-2005 19:59:16    10.94.163.153:00.00 Chassis ch
02-10-2005 20:47:41    ARP: Received ARP table from
02-10-2005 20:47:41    ARP: Received ARP table from
02-11-2005 00:01:50    ARP: Received ARP table from
02-11-2005 00:03:16    ARP: Received ARP table from
02-11-2005 00:05:13    ARP: Received ARP table from
```

Step 9 In this step, the transmittal of packets from Card 5, Port 1 is initiated, as shown in Figure 15-121:

Step A—Select the packet stream in Card 5, Port 1, and select the **Start Transmit** icon.

Figure 15-121 *Start Packet Stream from 5-1 to 5-2*



Line Rate 1,000 Mbps

Min 0 Max 100

Average

Total % Max Rate 10

Total Data Bit Rate 76.19 Mbps

Total Packets/Sec 148,809.52 fps

	Enable	Name	Flow	Control	Loop Count	Frame Size	Data Pattern Type
1	☑	2 - AutoGenerate	▭	End	1	64	Inc Byte

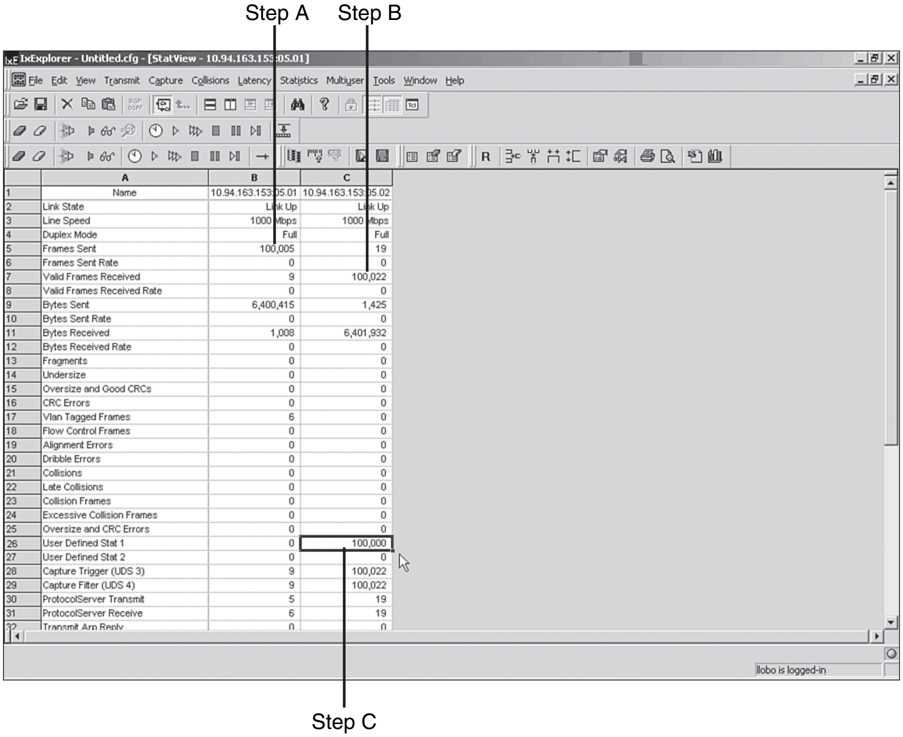
Step 10 A statistic window appears, as shown in Figure 15-122, if the **Auto-Open on Start-Transmit** check box is checked in **Tools > Options > Statistic Views**:

A—Shows the frames sent from 5-1.

B—Shows the frames received on 5-2.

C—Because B can show protocol packets as well, the UDF statistics show the correct count of packets received.

Figure 15-122 *Statistic Window*

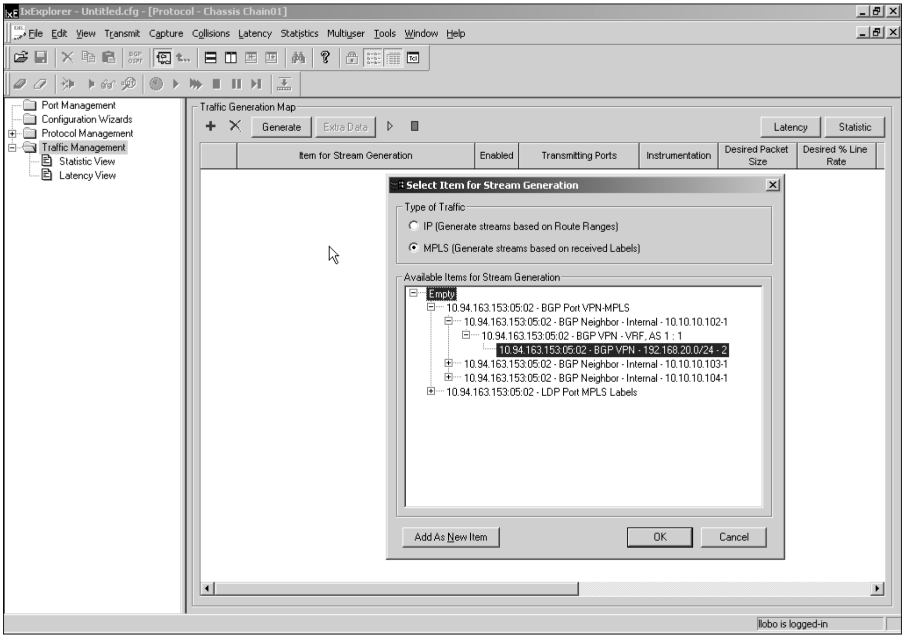

Step A
Step B
IxExplorer - Untitled.cfg - [StatView - 10.94.163.153:05.01]
File Edit View Transmit Capture Collisions Latency Statistics Multiuser Tools Window Help
llobo is logged-in
Step C

	A	B	C
1	Name	10.94.163.153:05.01	10.94.163.153:05.02
2	Link State	Link Up	Link Up
3	Line Speed	1000 Mbps	1000 Mbps
4	Duplex Mode	Full	Full
5	Frames Sent	100,005	19
6	Frames Sent Rate	0	0
7	Valid Frames Received	9	100,022
8	Valid Frames Received Rate	0	0
9	Bytes Sent	6,400,415	1,425
10	Bytes Sent Rate	0	0
11	Bytes Received	1,008	6,401,932
12	Bytes Received Rate	0	0
13	Fragments	0	0
14	Undersize	0	0
15	Oversize and Good CRCs	0	0
16	CRC Errors	0	0
17	Vlan Tagged Frames	6	0
18	Flow Control Frames	0	0
19	Alignment Errors	0	0
20	Dribble Errors	0	0
21	Collisions	0	0
22	Late Collisions	0	0
23	Collision Frames	0	0
24	Excessive Collision Frames	0	0
25	Oversize and CRC Errors	0	0
26	User Defined Stat 1	0	100,000
27	User Defined Stat 2	0	0
28	Capture Trigger (UDS 3)	9	100,022
29	Capture Filter (UDS 4)	9	100,022
30	ProtocolServer Transmit	5	19
31	ProtocolServer Receive	6	19
32	Transmit Arp Reply	0	0

CE2 to CE1

To generate traffic stream, follow the steps shown from CE1 to CE2, except Step 1. In Step 1, change the parameters as shown in Figure 15-123. The rest of the steps can be followed as shown.

Figure 15-123 *Traffic Map*



Select Item for Stream Generation

Type of Traffic

○ IP (Generate streams based on Route Ranges)

● MPLS (Generate streams based on received Labels)

Available Items for Stream Generation

```
⊟ Empty
    ⊟ 10.94.163.153:05:02 - BGP Port VPN-MPLS
        ⊟ 10.94.163.153:05:02 - BGP Neighbor - Internal - 10.10.10.102-1
            ⊟ 10.94.163.153:05:02 - BGP VPN - VRF, AS 1 : 1
                10.94.163.153:05:02 - BGP VPN - 192.168.20.0/24 - 2
        ⊞ 10.94.163.153:05:02 - BGP Neighbor - Internal - 10.10.10.103-1
        ⊞ 10.94.163.153:05:02 - BGP Neighbor - Internal - 10.10.10.104-1
    ⊞ 10.94.163.153:05:02 - LDP Port MPLS Labels
```

The statistic window when 5-1 and 5-2 are both transmitting is shown in Figure 15-124:

A—Frames sent from CE1 (5-1) to CE2 (5-2).

B—Frames sent from CE2 (5-2) to CE1 (5-1).

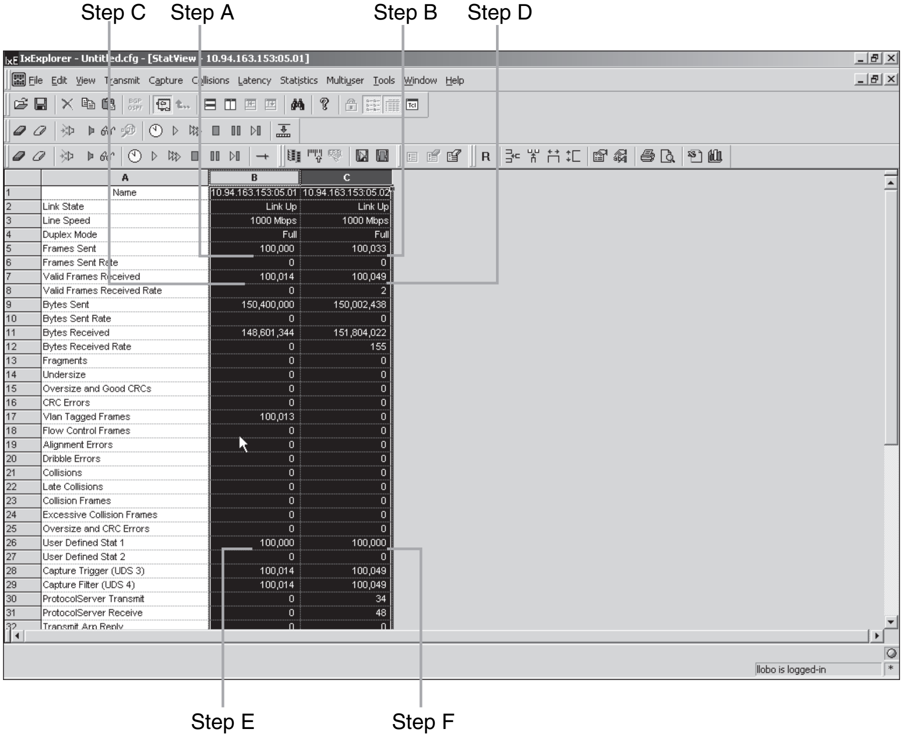
C—Frames received from CE2 (5-2) at CE1 (5-1).

D—Frames received from CE1 (5-1) at CE2 (5-2).

E—Accurate count of frames received from CE2 (5-2) at CE1 (5-1).

F—Accurate count of frames received from CE1 (5-1) at CE2 (5-2).

Figure 15-124 *Statistic Window*


Step C
Step A
Step B
Step D
IxExplorer - Untitled.cfg - [StatView - 10.94.163.153:05.01]
File Edit View Transmit Capture Collisions Latency Statistics Multiuser Tools Window Help
llobo is logged-in
Step E
Step F

	A	B	C
1	Name	10.94.163.153:05.01	10.94.163.153:05.02
2	Link State	Link Up	Link Up
3	Line Speed	1000 Mbps	1000 Mbps
4	Duplex Mode	Full	Full
5	Frames Sent	100,000	100,033
6	Frames Sent Rate	0	0
7	Valid Frames Received	100,014	100,049
8	Valid Frames Received Rate	0	2
9	Bytes Sent	150,400,000	150,002,438
10	Bytes Sent Rate	0	0
11	Bytes Received	148,601,344	151,804,022
12	Bytes Received Rate	0	155
13	Fragments	0	0
14	Undersize	0	0
15	Oversize and Good CRCs	0	0
16	CRC Errors	0	0
17	Vlan Tagged Frames	100,013	0
18	Flow Control Frames	0	0
19	Alignment Errors	0	0
20	Dribble Errors	0	0
21	Collisions	0	0
22	Late Collisions	0	0
23	Collision Frames	0	0
24	Excessive Collision Frames	0	0
25	Oversize and CRC Errors	0	0
26	User Defined Stat 1	100,000	100,000
27	User Defined Stat 2	0	0
28	Capture Trigger (UDS 3)	100,014	100,049
29	Capture Filter (UDS 4)	100,014	100,049
30	ProtocolServer Transmit	0	34
31	ProtocolServer Receive	0	48
32	Transmit Arp Reply	0	0

Example 15-18 displays the DUT configuration for MPLS VPN.

Example 15-18 *DUT Configuration for MPLS VPN*

```
hostname DUT
!
boot system flash disk2:c7200-p-mz.122-24.8.S2
!
ip subnet-zero
ip cef
!
ip vrf VRF-BGP
 rd 1:2
 route-target export 1:2
 route-target import 1:2
!
ip vrf VRF-OSPF
 rd 1:3
 route-target export 1:3
 route-target import 1:3
!
```

Example 15-18 *DUT Configuration for MPLS VPN (Continued)*

```
ip vrf VRF-RIP
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
mpls ldp router-id Loopback0
mpls label protocol ldp
!
interface Loopback0
 ip address 10.10.10.101 255.255.255.255
!
interface GigabitEthernet0/1
 duplex full
 speed auto
 media-type gbic
 negotiation auto
!
interface GigabitEthernet0/1.100
 encapsulation dot1Q 100
 ip vrf forwarding VRF-RIP
 ip address 172.16.1.2 255.255.255.252
!
interface GigabitEthernet0/1.101
 encapsulation dot1Q 101
 ip vrf forwarding VRF-BGP
 ip address 172.16.2.2 255.255.255.252
!
interface GigabitEthernet0/1.102
 encapsulation dot1Q 102
 ip vrf forwarding VRF-OSPF
 ip address 172.16.3.2 255.255.255.252
!
interface GigabitEthernet0/2
 description connected to IXIA (PE2) port 5-2
  ip address 10.10.10.1 255.255.255.252
  duplex auto
  speed auto
  media-type gbic
  negotiation auto
  mpls ip
  no clns route-cache
!
router ospf 102 vrf VRF-OSPF
 log-adjacency-changes
 redistribute bgp 1 metric 1 subnets
 network 172.16.3.0 0.0.0.255 area 0
!
router ospf 1
 log-adjacency-changes
 network 10.10.10.0 0.0.0.255 area 0
!
```

continues

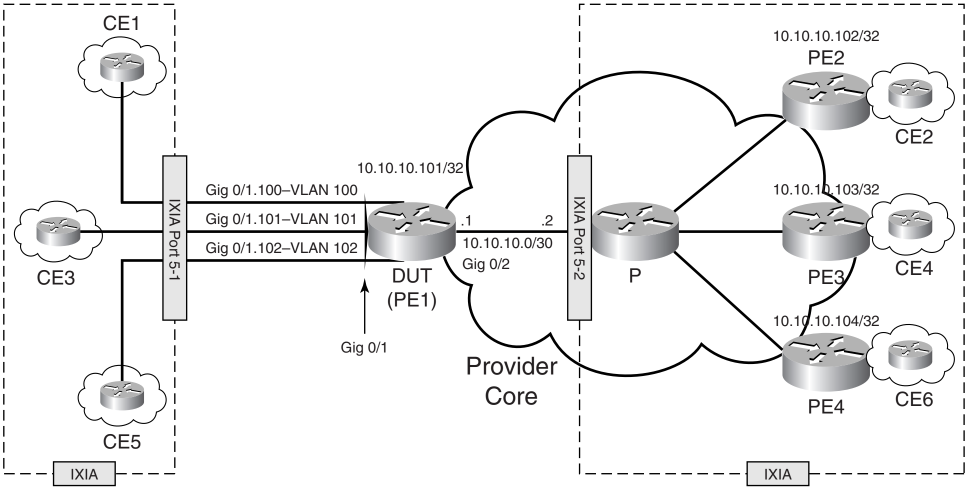
Example 15-18 *DUT Configuration for MPLS VPN (Continued)*

```
router rip
 version 2
 !
 address-family ipv4 vrf VRF-RIP
 redistribute bgp 1 metric transparent
 network 172.16.0.0
 no auto-summary
 exit-address-family
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.10.10.102 remote-as 1
 neighbor 10.10.10.102 update-source Loopback0
 neighbor 10.10.10.103 remote-as 1
 neighbor 10.10.10.103 update-source Loopback0
 neighbor 10.10.10.104 remote-as 1
 neighbor 10.10.10.104 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 10.10.10.102 activate
 neighbor 10.10.10.102 send-community extended
 neighbor 10.10.10.103 activate
 neighbor 10.10.10.103 send-community extended
 neighbor 10.10.10.104 activate
 neighbor 10.10.10.104 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf VRF-RIP
 redistribute rip metric 1
 no auto-summary
 no synchronization
 exit-address-family
 !
  address-family ipv4 vrf VRF-OSPF
  redistribute ospf 102 vrf VRF-OSPF
  no auto-summary
  no synchronization
  exit-address-family
  !
  address-family ipv4 vrf VRF-BGP
  neighbor 172.16.2.1 remote-as 65001
  neighbor 172.16.2.1 activate
  no auto-summary
  no synchronization
  exit-address-family
!
ip classless
```

Testing L2 VPN with IXIA

Figure 15-125 shows an L2 VPN network. The VC IDs used on the VLAN sub-interfaces are 100, 101, and 102. The steps to configure L2 VPN for the IXIA simulated network are shown in the following subsections.

Figure 15-125 *L2 VPN Test Network*



Configuring L2 VPN on IXIA

Before configuring the following, MPLS must already be enabled on the IXIA. Refer to the section "Basic MPLS Configuration Procedure on IXIA" in this chapter.

The steps to configure L2 VPN are

Step 1 In this step, the LDP routers are defined so that the Martini session can be formed with the DUT, as displayed in Figure 15-126:

Step A—In the Protocol window, select **Card 5, Port 2** under the LDP folder.

Step B—Select the **Router** tab in the right pane and click it three times to create three additional LDP routers.

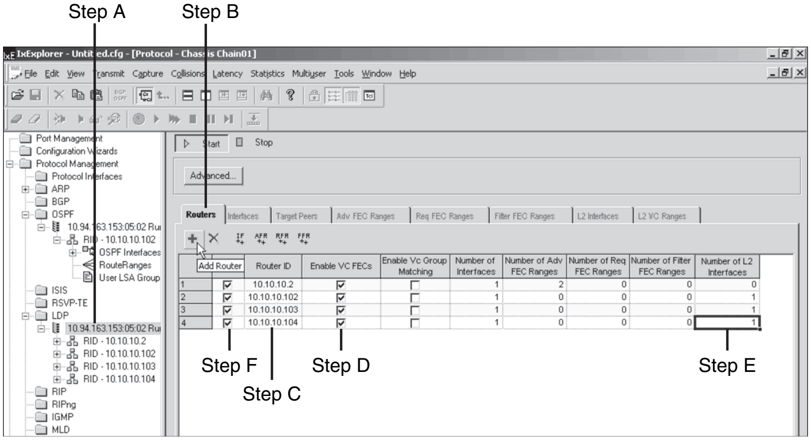
Step C—Configure the router IDs for each LDP router created.

Step D—Ensure that the Enable VC FECs box is checked.

Step E—Configure the number of L2 interfaces for each LDP router as "1."

Step F—Enable the LDP routers.

Figure 15-126 *Configure LDP Routers*



		Router ID	Enable VC FECs	Enable Vc Group Matching	Number of Interfaces	Number of Adv FEC Ranges	Number of Req FEC Ranges	Number of Filter FEC Ranges	Number of L2 Interfaces
1	☑	10.10.10.2	☑	☐	1	2	0	0	0
2	☑	10.10.10.102	☑	☐	1	0	0	0	1
3	☑	10.10.10.103	☑	☐	1	0	0	0	1
4	☑	10.10.10.104	☑	☐	1	0	0	0	1

Step 2 In this step, the LDP interfaces are defined as displayed in Figure 15-127:

Step A—Select the **Interfaces** tab.

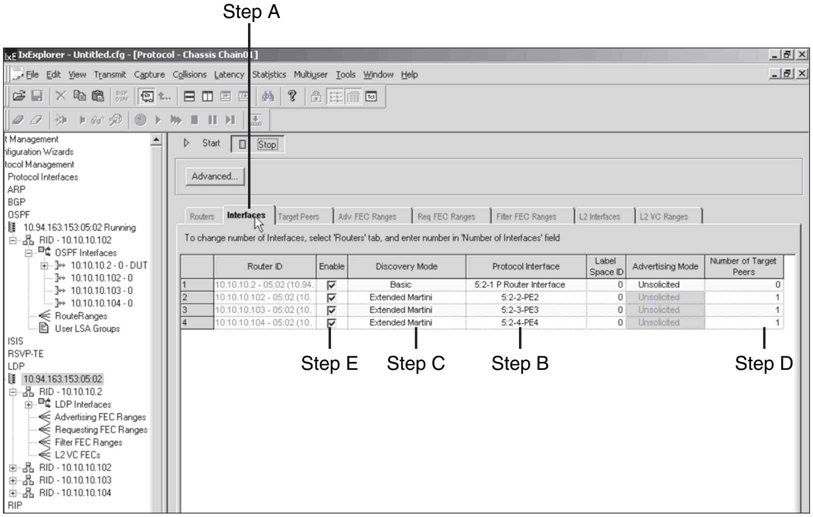
Step B—Select the protocol interface for PE2, PE3, and PE4.

Step C—Select **Extended Martini** as the LDP discovery mode.

Step D—Configure the number of LDP targeted peers for each LDP router as "1."

Step E—Enable the LDP interfaces.

Figure 15-127 *Configure LDP Interfaces*



To change number of Interfaces, select 'Routers' tab, and enter number in 'Number of Interfaces' field

	Router ID	Enable	Discovery Mode	Protocol Interface	Label Space ID	Advertising Mode	Number of Target Peers
1	10.10.10.2 - 05:02 (10.94.	☑	Basic	5:2-1 P Router Interface	0	Unsolicited	0
2	10.10.10.102 - 05:02 (10.	☑	Extended Martini	5:2-2-PE2	0	Unsolicited	1
3	10.10.10.103 - 05:02 (10.	☑	Extended Martini	5:2-3-PE3	0	Unsolicited	1
4	10.10.10.104 - 05:02 (10.	☑	Extended Martini	5:2-4-PE4	0	Unsolicited	1

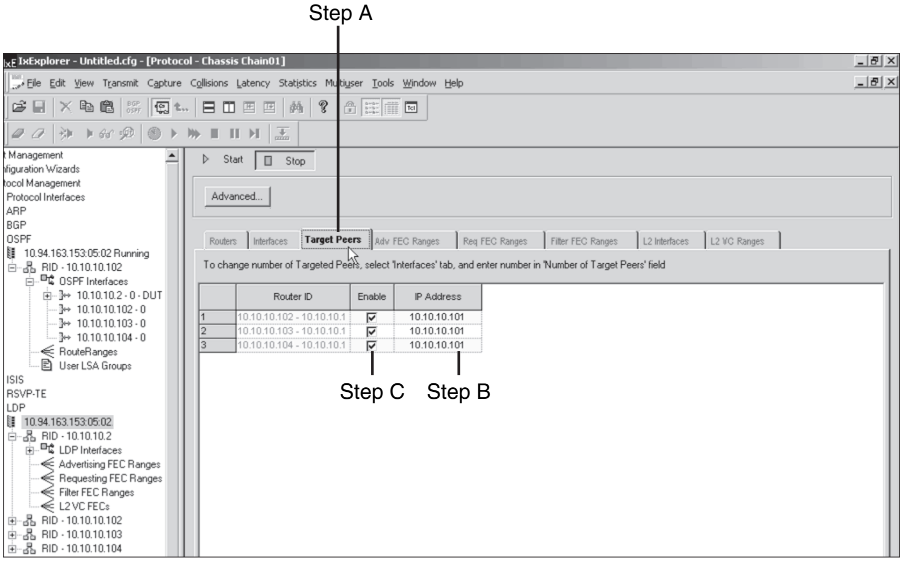
Step 3 In this step, define the LDP target peers as displayed in Figure 15-128:

Step A—Select the **Target Peers** tab.

Step B—Configure the target peer IP address as 10.10.10.101, which is the loopback on the DUT.

Step C—Enable the target peers.

Figure 15-128 *Configure LDP Target Peers*


Step A
IxExplorer - Untitled.cfg - [Protocol - Chassis Chain01]
File Edit View Transmit Capture Collisions Latency Statistics Multiuser Tools Window Help
Start
Stop
Advanced...
Routers
Interfaces
Target Peers
Adv FEC Ranges
Req FEC Ranges
Filter FEC Ranges
L2 Interfaces
L2 VC Ranges
Step C
Step B

To change number of Targeted Peers, select 'Interfaces' tab, and enter number in 'Number of Target Peers' field

	Router ID	Enable	IP Address
1	10.10.10.102 - 10.10.10.1	☑	10.10.10.101
2	10.10.10.103 - 10.10.10.1	☑	10.10.10.101
3	10.10.10.104 - 10.10.10.1	☑	10.10.10.101

Step 4 In this step, the L2 interfaces are defined as displayed in Figure 15-129:

Step A—Select the **L2 Interfaces** tab.

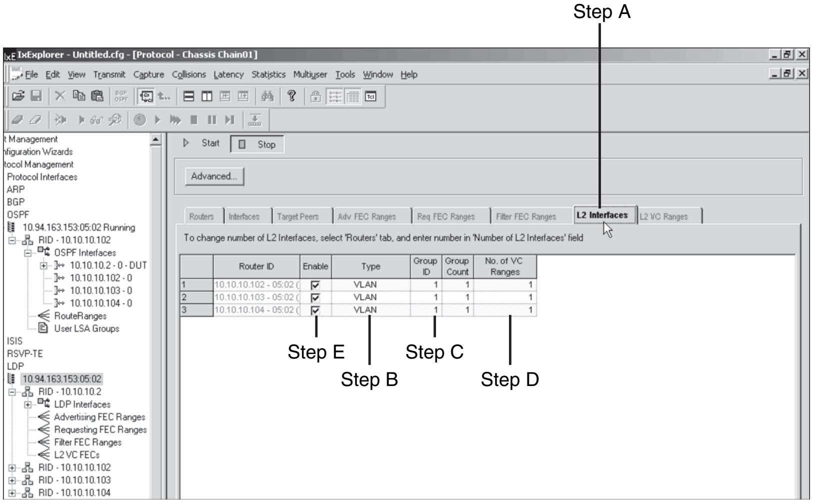
Step B—Select the VC type as Ethernet VLAN.

Step C—Configure the group ID as 1.

Step D—Configure L2 VC ranges for each LDP router as "1."

Step E—Enable the L2 interfaces.

Figure 15-129 *Configure L2 Interfaces*



To change number of L2 Interfaces, select 'Routers' tab, and enter number in 'Number of L2 Interfaces' field

	Router ID	Enable	Type	Group ID	Group Count	No. of VC Ranges
1	10.10.10.102 - 05:02 (	☑	VLAN	1	1	1
2	10.10.10.103 - 05:02 (	☑	VLAN	1	1	1
3	10.10.10.104 - 05:02 (	☑	VLAN	1	1	1

Step 5 In this step, the L2 VC range is defined:

Step A—Select the **L2 VC Ranges** tab.

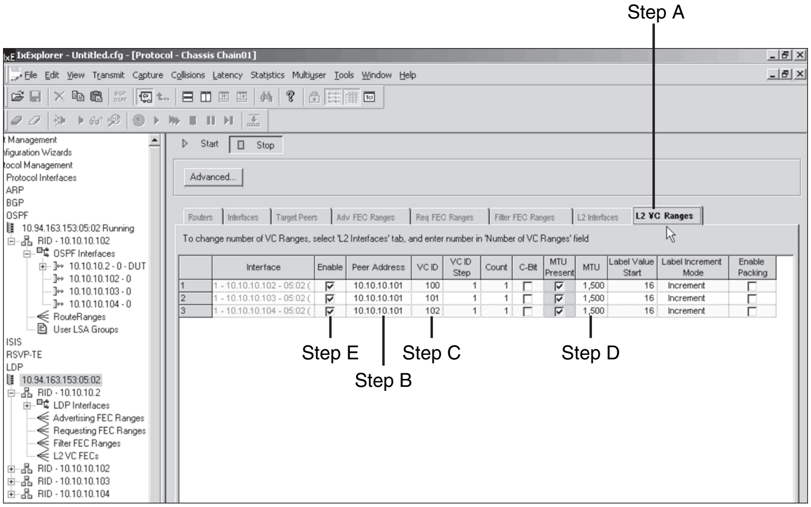
Step B—Configure the DUT (10.10.10.101) as the peer.

Step C—Configure the VC ID as shown in Figure 15-130.

Step D—Configure the MTU as 1,500.

Step E—Enable the L2 VC range and start the LDP sessions by clicking the **Start** icon.

Figure 15-130 *Configure L2 VC Range*



To change number of VC Ranges, select 'L2 Interfaces' tab, and enter number in 'Number of VC Ranges' field

	Interface	Enable	Peer Address	VC ID	VC ID Step	Count	C-Bit	MTU Present	MTU	Label Value Start	Label Increment Mode	Enable Packing
1	1 - 10.10.10.102 - 05:02 (	☑	10.10.10.101	100	1	1	☐	☑	1,500	16	Increment	☐
2	1 - 10.10.10.103 - 05:02 (	☑	10.10.10.101	101	1	1	☐	☑	1,500	16	Increment	☐
3	1 - 10.10.10.104 - 05:02 (	☑	10.10.10.101	102	1	1	☐	☑	1,500	16	Increment	☐

Verify L2 VPN on IXIA

The steps to verify the L2 VPN are

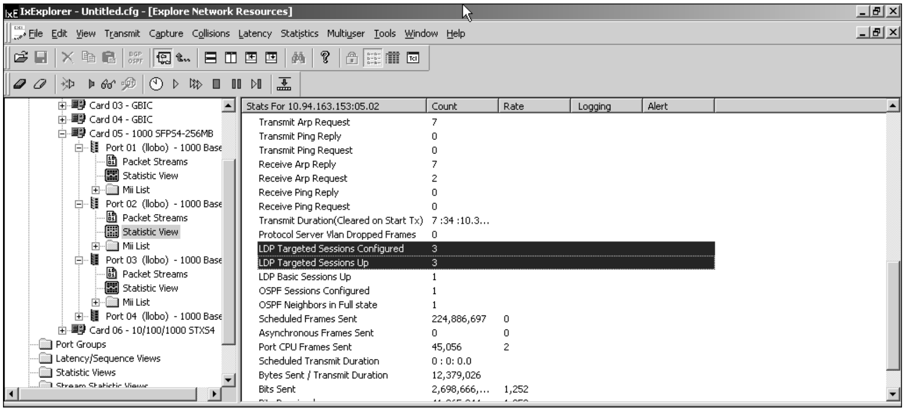
Step 1 On the DUT, verify by issuing **show mpls l2transport vc**. Example 15-19 shows the output of **show mpls l2transport vc** on the DUT.

Example 15-19 **show mpls l2transport vc**

```
DUT#show MPLS l2transport vc

Local intf     Local circuit        Dest address    VC ID      Status
-------------  -------------------- --------------- ---------- ----------
Gi0/1.100      Eth VLAN 100         10.10.10.102    100        UP
Gi0/1.101      Eth VLAN 101         10.10.10.103    101        UP
Gi0/1.102      Eth VLAN 102         10.10.10.104    102        UP
```

Step 2 You can verify the same on the IXIA by clicking the **Statistic View** on the IXIA for Port 5-2. Figure 15-131 shows that the targeted LDP sessions are up and running.

Figure 15-131 *Verify Targeted LDP Sessions*


IxExplorer - Untitled.cfg - [Explore Network Resources]
File Edit View Transmit Capture Collisions Latency Statistics Multiuser Tools Window Help
Card 03 - GBIC
Card 04 - GBIC
Card 05 - 1000 SFPS4-256MB
Port 01 (llobo) - 1000 Base
Packet Streams
Statistic View
Mii List
Port 02 (llobo) - 1000 Base
Packet Streams
Statistic View
Mii List
Port 03 (llobo) - 1000 Base
Packet Streams
Statistic View
Mii List
Port 04 (llobo) - 1000 Base
Card 06 - 10/100/1000 STXS4
Port Groups
Latency/Sequence Views
Statistic Views

Stats For 10.94.163.153:05.02	Count	Rate	Logging	Alert
Transmit Arp Request	7			
Transmit Ping Reply	0			
Transmit Ping Request	0			
Receive Arp Reply	7			
Receive Arp Request	2			
Receive Ping Reply	0			
Receive Ping Request	0			
Transmit Duration(Cleared on Start Tx)	7 :34 :10.3...			
Protocol Server Vlan Dropped Frames	0			
LDP Targeted Sessions Configured	3			
LDP Targeted Sessions Up	3			
LDP Basic Sessions Up	1			
OSPF Sessions Configured	1			
OSPF Neighbors in Full state	1			
Scheduled Frames Sent	224,886,697	0		
Asynchronous Frames Sent	0	0		
Port CPU Frames Sent	45,056	2		
Scheduled Transmit Duration	0 : 0: 0.0			
Bytes Sent / Transmit Duration	12,379,026			
Bits Sent	2,698,666,...	1,252		

L2 VPN Traffic Generation on IXIA

In this section, traffic will be generated on VC ID 100 originating from 10.10.10.102 to 10.10.10.101.

Generate Traffic from Card 5, Port 2

The following steps outline the procedure for traffic generation from IXIA Port 5-2:

Step 1 The steps are as follows:

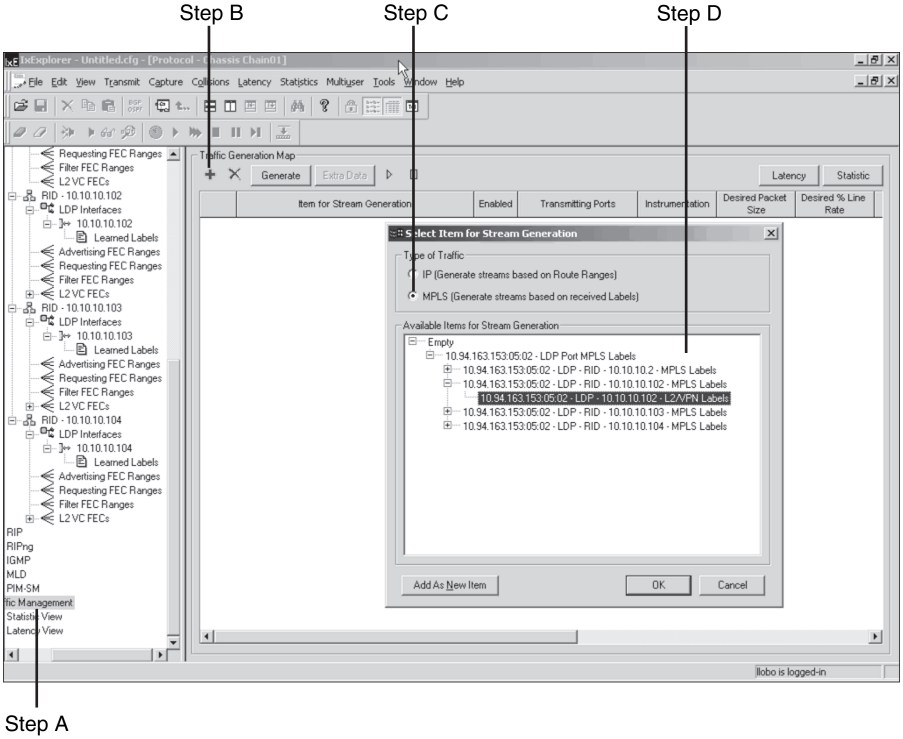
Step A—In the Protocol window, click the **Traffic Management** folder.

Step B—Click the **plus** icon and a Select Item for Stream Generation dialog appears.

Step C—Select **MPLS**.

Step D—Select the destination by expanding the 5-2 LDP folder for 10.10.10.102, and select the appropriate source, as shown in Figure 15-132.

Figure 15-132 *Configure Traffic Stream from 10.10.10.102 to CE1 on Port 5-2*



Type of Traffic

○ IP (Generate streams based on Route Ranges)

● MPLS (Generate streams based on received Labels)

Available Items for Stream Generation

- Empty
  - 10.94.163.153:05:02 - LDP Port MPLS Labels
    - 10.94.163.153:05:02 - LDP - RID - 10.10.10.2 - MPLS Labels
    - 10.94.163.153:05:02 - LDP - RID - 10.10.10.102 - MPLS Labels
      - 10.94.163.153:05:02 - LDP - 10.10.10.102 - L2/VPN Labels
    - 10.94.163.153:05:02 - LDP - RID - 10.10.10.103 - MPLS Labels
    - 10.94.163.153:05:02 - LDP - RID - 10.10.10.104 - MPLS Labels

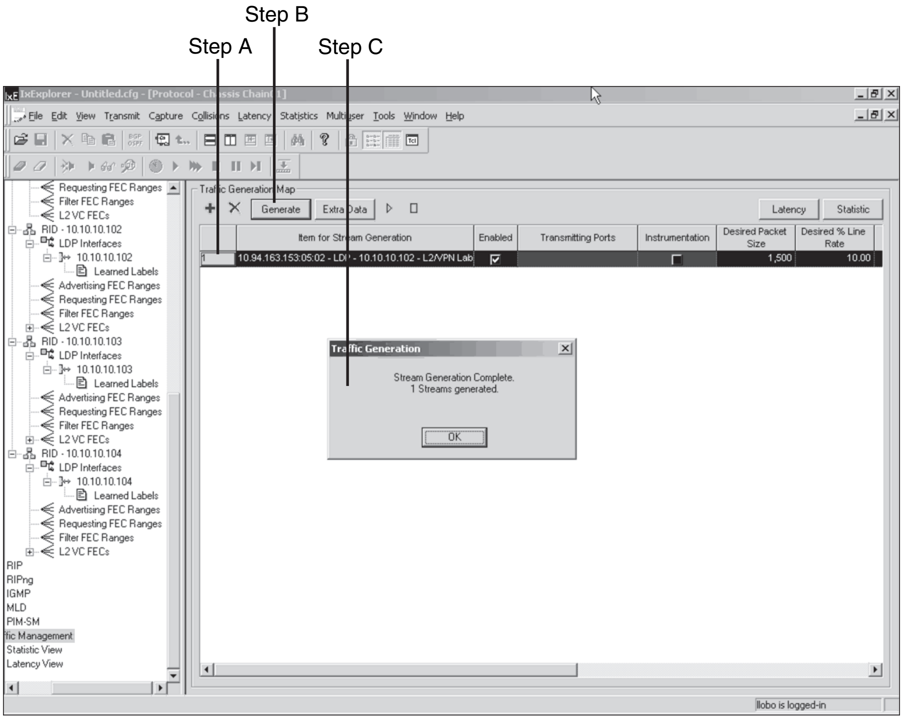
Step 2 The steps displayed in Figure 15-133 are as follows:

Step A—Select the traffic map.

Step B—Click the **Generate** button.

Step C—A dialog box indicating the stream is generated appears. Click **OK**.

Figure 15-133 *Generate the Traffic Stream*



	Item for Stream Generation	Enabled	Transmitting Ports	Instrumentation	Desired Packet Size	Desired % Line Rate
1	10.94.163.153:05:02 - LDP - 10.10.10.102 - L2VPN Lab	☑		☐	1,500	10.00

Traffic Generation

Stream Generation Complete.
1 Streams generated.

OK

Generate Traffic from Card 5, Port 1

The following steps outline the procedure for traffic generation from the IXIA Port 5-1:

Step 1 In this step, you will create a traffic stream under Port 5-1. Select **Packet Streams** under Card 5, Port 1, as displayed in Figure 15-134:

Step A—Right-click and select **New Stream**.

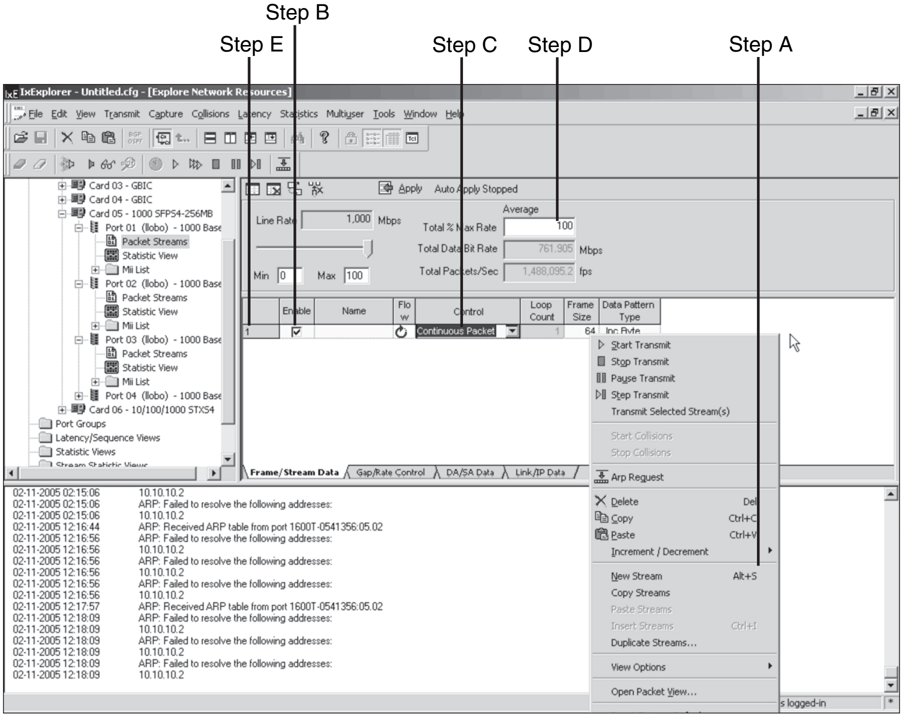
Step B—Enable the stream.

Step C—Select **End**.

Step D—Change max rate to be 10 percent from the default 100 percent.

Step E—Select the stream and then double-click it.

Figure 15-134 *Create Traffic Stream On*



Line Rate 1,000 Mbps

Min 0 Max 100

Average

Total % Max Rate 100

Total Data Bit Rate 761.905 Mbps

Total Packets/Sec 1,488,095.2 fps

	Enable	Name	Flow	Control	Loop Count	Frame Size	Data Pattern Type
1	☑			Continuous Packet	1	64	Inc Byte

```
02-11-2005 02:15:06    10.10.10.2
02-11-2005 02:15:06    ARP: Failed to resolve the following addresses:
02-11-2005 02:15:06    10.10.10.2
02-11-2005 12:16:44    ARP: Received ARP table from port 1600T-0541356:05.02
02-11-2005 12:16:56    ARP: Failed to resolve the following addresses:
02-11-2005 12:16:56    10.10.10.2
02-11-2005 12:16:56    ARP: Failed to resolve the following addresses:
02-11-2005 12:16:56    10.10.10.2
02-11-2005 12:16:56    ARP: Failed to resolve the following addresses:
02-11-2005 12:16:56    10.10.10.2
02-11-2005 12:17:57    ARP: Received ARP table from port 1600T-0541356:05.02
02-11-2005 12:18:09    ARP: Failed to resolve the following addresses:
02-11-2005 12:18:09    10.10.10.2
02-11-2005 12:18:09    ARP: Failed to resolve the following addresses:
02-11-2005 12:18:09    10.10.10.2
02-11-2005 12:18:09    ARP: Failed to resolve the following addresses:
02-11-2005 12:18:09    10.10.10.2
```

Step 2 In this step, configure the stream properties as displayed in Figure 15-135:

Step A—Select the **Stream Control** tab.

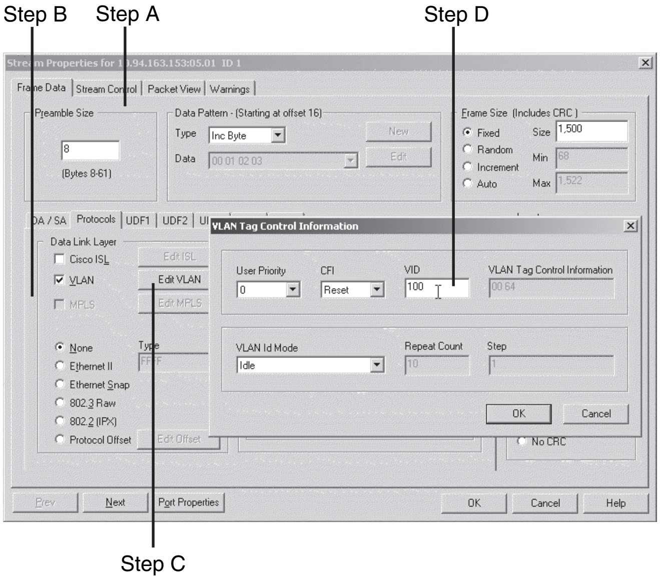
Step B—Enable the VLAN check box.

Step C—Click the **Edit VLAN** button.

Step D—Change the VLAN ID to 100.

Optionally, you can change the packet count to 100,000.

Figure 15-135 *Define Traffic Stream Properties*



Preamble Size: 8 (Bytes 8-61)

Data Pattern - (Starting at offset 16): Type: Inc Byte; Data: 00 01 02 03

Frame Size (Includes CRC): ● Fixed ○ Random ○ Increment ○ Auto; Size: 1,500; Min: 68; Max: 1,522

Data Link Layer: ☐ Cisco ISL ☑ VLAN ☐ MPLS

● None ○ Ethernet II ○ Ethernet Snap ○ 802.3 Raw ○ 802.2 (IPX) ○ Protocol Offset; Type: FFFF

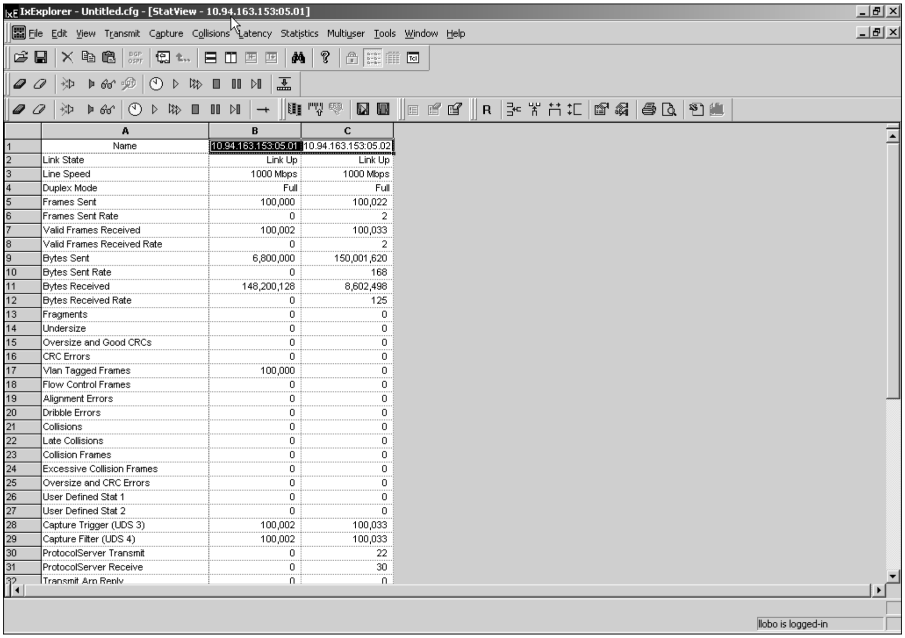
○ No CRC

VLAN Tag Control Information: User Priority: 0; CFI: Reset; VID: 100; VLAN Tag Control Information: 00 64

VLAN Id Mode: Idle; Repeat Count: 10; Step: 1

Figure 15-136 shows the statistic views when streams are generated on 5-1 and 5-2.

Figure 15-136 *Define Traffic Stream Properties*



IxExplorer - Untitled.cfg - [StatView - 10.94.163.153:05.01]
File Edit View Transmit Capture Collisions Latency Statistics Multiuser Tools Window Help
llobo is logged-in

	A	B	C
1	Name	10.94.163.153:05.01	10.94.163.153:05.02
2	Link State	Link Up	Link Up
3	Line Speed	1000 Mbps	1000 Mbps
4	Duplex Mode	Full	Full
5	Frames Sent	100,000	100,022
6	Frames Sent Rate	0	2
7	Valid Frames Received	100,002	100,033
8	Valid Frames Received Rate	0	2
9	Bytes Sent	6,800,000	150,001,620
10	Bytes Sent Rate	0	168
11	Bytes Received	148,200,128	8,602,498
12	Bytes Received Rate	0	125
13	Fragments	0	0
14	Undersize	0	0
15	Oversize and Good CRCs	0	0
16	CRC Errors	0	0
17	Vlan Tagged Frames	100,000	0
18	Flow Control Frames	0	0
19	Alignment Errors	0	0
20	Dribble Errors	0	0
21	Collisions	0	0
22	Late Collisions	0	0
23	Collision Frames	0	0
24	Excessive Collision Frames	0	0
25	Oversize and CRC Errors	0	0
26	User Defined Stat 1	0	0
27	User Defined Stat 2	0	0
28	Capture Trigger (UDS 3)	100,002	100,033
29	Capture Filter (UDS 4)	100,002	100,033
30	ProtocolServer Transmit	0	22
31	ProtocolServer Receive	0	30
32	Transmit Arp Reply	0	0

Example 15-20 displays the L2 VPN DUT configuration.

Example 15-20 *DUT Configuration—L2 VPN*

```
!
hostname DUT
!
boot-start-marker
boot system flash disk2:c7200-p-mz.122-24.8.S2
boot-end-marker
!
!
ip subnet-zero
ip cef
!
!
!
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp router-id Loopback0
mpls label protocol ldp
!
interface Loopback0
 ip address 10.10.10.101 255.255.255.255
 no clns route-cache
!
!
!
interface GigabitEthernet0/1
 no ip address
 duplex full
 speed auto
 media-type gbic
 negotiation auto
 no clns route-cache
!
interface GigabitEthernet0/1.100
 encapsulation dot1Q 100
 no cdp enable
 xconnect 10.10.10.102 100 encapsulation mpls
!
interface GigabitEthernet0/1.101
 encapsulation dot1Q 101
 no cdp enable
 xconnect 10.10.10.103 101 encapsulation mpls
!
interface GigabitEthernet0/1.102
 encapsulation dot1Q 102
 no cdp enable
 xconnect 10.10.10.104 102 encapsulation mpls
!
interface GigabitEthernet0/2
 description connected to IXIA (PE2) port 5-2
 ip address 10.10.10.1 255.255.255.252
 duplex auto
```

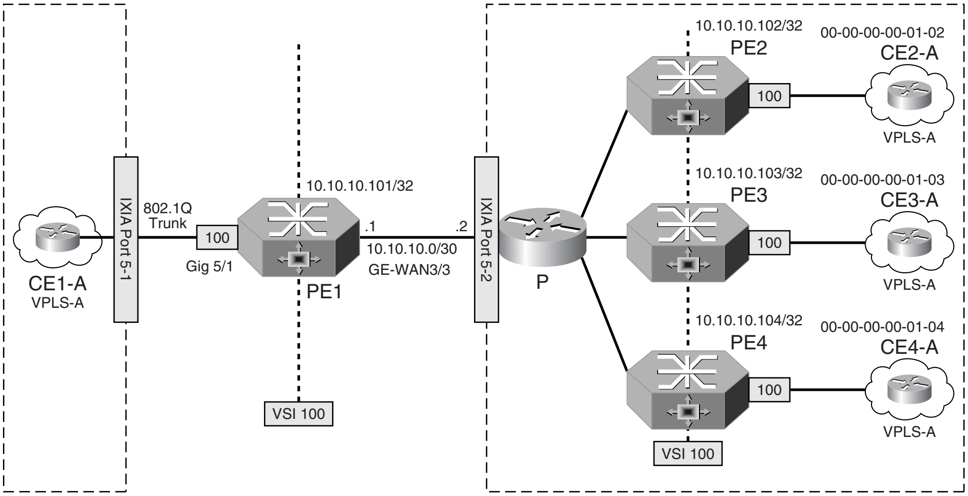
Example 15-20 *DUT Configuration—L2 VPN (Continued)*

```
 speed auto
 media-type gbic
 negotiation auto
 mpls ip
 no clns route-cache
!
!
router ospf 1
 log-adjacency-changes
 network 10.10.10.0 0.0.0.255 area 0
```

Testing VPLS with IXIA

Figure 15-137 shows a VPLS network. In this network, all the remote CE devices are provisioned as part of the same broadcast domain.

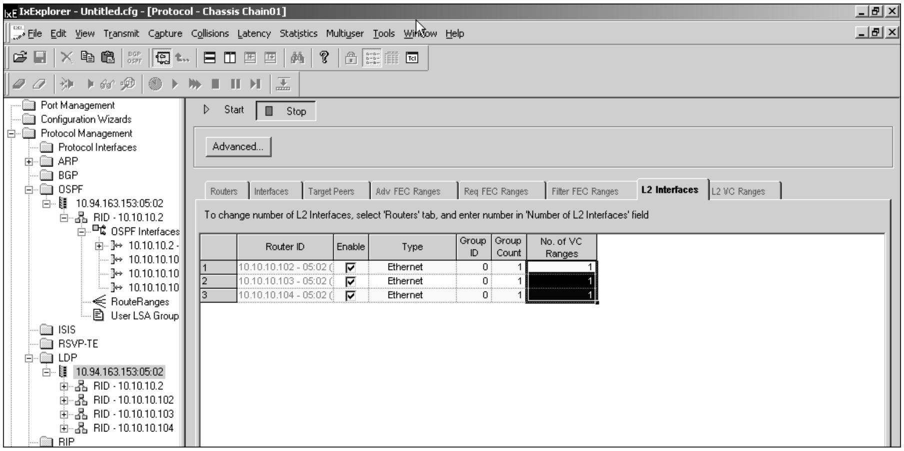
Figure 15-137 *VPLS Test Network*



Configuring VPLS with IXIA

Steps 1 to 3 in the section "Configuring L2 VPN on IXIA" are common to configuring VPLS. For VPLS, in Step 4 of "Configuring L2 VPN on IXIA," change the type to Ethernet. This is shown in Figure 15-138.

Figure 15-138 *Configuring L2 Interfaces in VPLS*

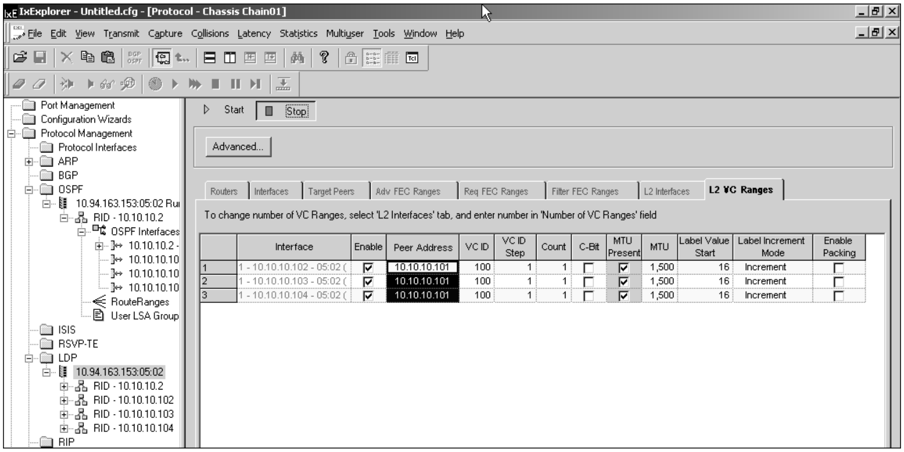


To change number of L2 Interfaces, select 'Routers' tab, and enter number in 'Number of L2 Interfaces' field

	Router ID	Enable	Type	Group ID	Group Count	No. of VC Ranges
1	10.10.10.102 - 05:02 (	☑	Ethernet	0	1	1
2	10.10.10.103 - 05:02 (	☑	Ethernet	0	1	1
3	10.10.10.104 - 05:02 (	☑	Ethernet	0	1	1

Step 5 remains the same for VPLS as shown in "Configuring L2 VPN on IXIA" except that the VC ID is changed to 100 for all PE routers. This is shown in Figure 15-139.

Figure 15-139 *Configuring L2 VC Ranges in VPLS*



To change number of VC Ranges, select 'L2 Interfaces' tab, and enter number in 'Number of VC Ranges' field

	Interface	Enable	Peer Address	VC ID	VC ID Step	Count	C-Bit	MTU Present	MTU	Label Value Start	Label Increment Mode	Enable Packing
1	1 - 10.10.10.102 - 05:02 (	☑	10.10.10.101	100	1	1	☐	☑	1,500	16	Increment	☐
2	1 - 10.10.10.103 - 05:02 (	☑	10.10.10.101	100	1	1	☐	☑	1,500	16	Increment	☐
3	1 - 10.10.10.104 - 05:02 (	☑	10.10.10.101	100	1	1	☐	☑	1,500	16	Increment	☐

Verify VPLS on IXIA

On the DUT, verify by issuing **show mpls l2transport vc**. Example 15-21 shows the output of **show mpls l2transport vc** on the DUT.

Example 15-21 **show mpls l2transport vc** *on DUT*

```
DUT#show mpls l2transport vc

Local intf     Local circuit        Dest address    VC ID      Status
-------------  -------------------- --------------- ---------- ----------
VFI VPLS-A     VFI                  10.10.10.102    100        UP
VFI VPLS-A     VFI                  10.10.10.103    100        UP
VFI VPLS-A     VFI                  10.10.10.104    100        UP
DUT#show mpls ldp neighbor
    Peer LDP Ident: 10.10.10.104:0; Local LDP Ident 10.10.10.101:0
        TCP connection: 10.10.10.104.32835 - 10.10.10.101.646
        State: Oper; Msgs sent/rcvd: 11/5; Downstream
        Up time: 00:00:18
        LDP discovery sources:
          Targeted Hello 10.10.10.101 -> 10.10.10.104, active, passive
        Addresses bound to peer LDP Ident:
          10.10.10.104
    Peer LDP Ident: 10.10.10.2:0; Local LDP Ident 10.10.10.101:0
        TCP connection: 10.10.10.2.646 - 10.10.10.101.11087
        State: Oper; Msgs sent/rcvd: 9/7; Downstream
        Up time: 00:00:11
        LDP discovery sources:
          GE-WAN3/3, Src IP addr: 10.10.10.2
        Addresses bound to peer LDP Ident:
          10.10.10.2
    Peer LDP Ident: 10.10.10.103:0; Local LDP Ident 10.10.10.101:0
        TCP connection: 10.10.10.103.32836 - 10.10.10.101.646
        State: Oper; Msgs sent/rcvd: 9/4; Downstream
        Up time: 00:00:08
        Addresses bound to peer LDP Ident:
          10.10.10.103
    Peer LDP Ident: 10.10.10.102:0; Local LDP Ident 10.10.10.101:0
        TCP connection: 10.10.10.102.32837 - 10.10.10.101.646
        State: Oper; Msgs sent/rcvd: 10/4; Downstream
        Up time: 00:00:08
        Addresses bound to peer LDP Ident:
          10.10.10.102
```

Verification on the IXIA is the same as what's shown in Step 2 of the section "Verify L2 VPN on IXIA."

Traffic Generation

In this section, traffic is generated on VC ID 100 originating from 10.10.10.102 to 10.10.10.101.

Generate Traffic from Card 5, Port 2

The following steps outline the procedure for traffic generation from IXIA Port 5-2:

Step 1 This step is the same as what's shown in the section, "Generate Traffic from Card 5, Port 1."

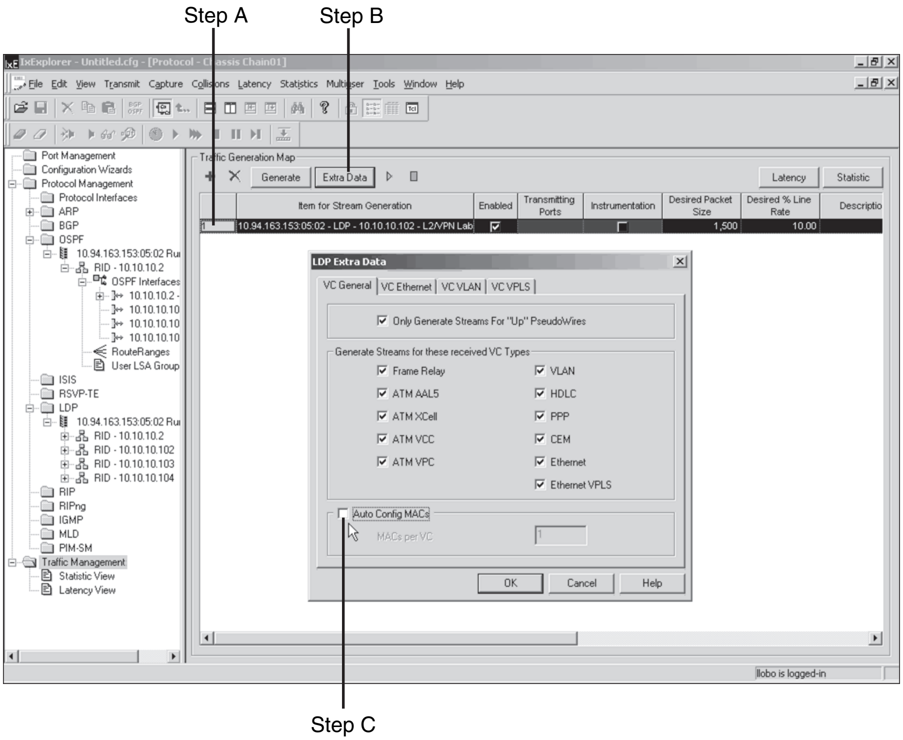
Step 2 Configure the desired packet size and rate and then use these steps, as displayed in Figure 15-140.

Step A—Select the traffic map.

Step B—Click the **Extra Data** button.

Step C—A dialog box, LDP Extra Data, appears. Remove the check mark from the **Auto-Config MACs** field.

Figure 15-140 *Configure Ethernet Data*



	Item for Stream Generation	Enabled	Transmitting Ports	Instrumentation	Desired Packet Size	Desired % Line Rate	Descriptio
1	10.94.163.153:05:02 - LDP - 10.10.10.102 - L2VPN Lab	☑		☐	1,500	10.00	

☑ Only Generate Streams For "Up" PseudoWires

Generate Streams for these received VC Types

☑ Frame Relay ☑ VLAN
☑ ATM AAL5 ☑ HDLC
☑ ATM XCell ☑ PPP
☑ ATM VCC ☑ CEM
☑ ATM VPC ☑ Ethernet
☑ Ethernet VPLS

☐ Auto Config MACs
MACs per VC 1

Step 3 Configure the desired packet size and rate and then use these steps, as displayed in Figure 15-141:

Step A—Select the **VC Ethernet** tab.

Step B—Define the SA to be CE2 MAC address 00-00-00-00-01-02.

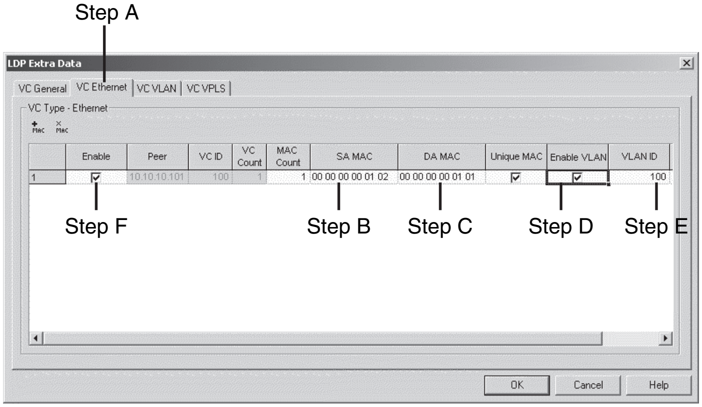
Step C—Define the DA to be CE1 MAC address 00-00-00-00-01-01. Ensure that the MAC address for CE1 in protocol interface is 00-00-00-00-01-01.

Step D—Enable the **VLAN** checkbox.

Step E—Configure the VLAN ID as 100.

Step F—Check the **Enable** box.

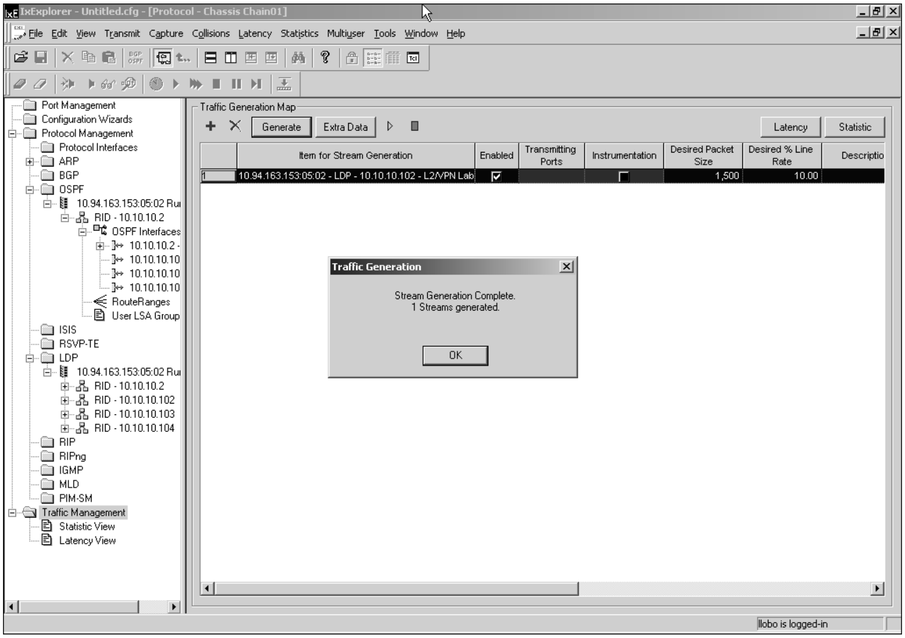
Figure 15-141 *Configure VC Ethernet Properties*



	Enable	Peer	VC ID	VC Count	MAC Count	SA MAC	DA MAC	Unique MAC	Enable VLAN	VLAN ID
1	☑	10.10.10.101	100	1	1	00 00 00 00 01 02	00 00 00 00 01 01	☑	☑	100

Step 4 Finally, generate the stream by clicking the **Generate** button shown in Figure 15-142. Configure the stream properties as shown earlier in the L3VPN Traffic generation on IXIA section. Generate the traffic stream by going to the **Explore Network Resources** window and clicking the **Start Transmit** button after selecting the appropriate traffic streams.

Figure 15-142 *Generate Traffic Stream*



	Item for Stream Generation	Enabled	Transmitting Ports	Instrumentation	Desired Packet Size	Desired % Line Rate	Descriptio
1	10.94.163.153:05:02 - LDP - 10.10.10.102 - L2VPN Lab	☑		☐	1,500	10.00	

Stream Generation Complete.
1 Streams generated.

Optionally, if packet signatures need to be introduced, use the following steps:

Step 1 Configure the desired packet size and rate, and then use these steps:

Step A—Select the stream and then double-click the stream for 5-2 to go to the pop-up window shown in Figure 15-143. Select **UDF5** in the Frame Data tab.

Step B—Configure the offset to 100.

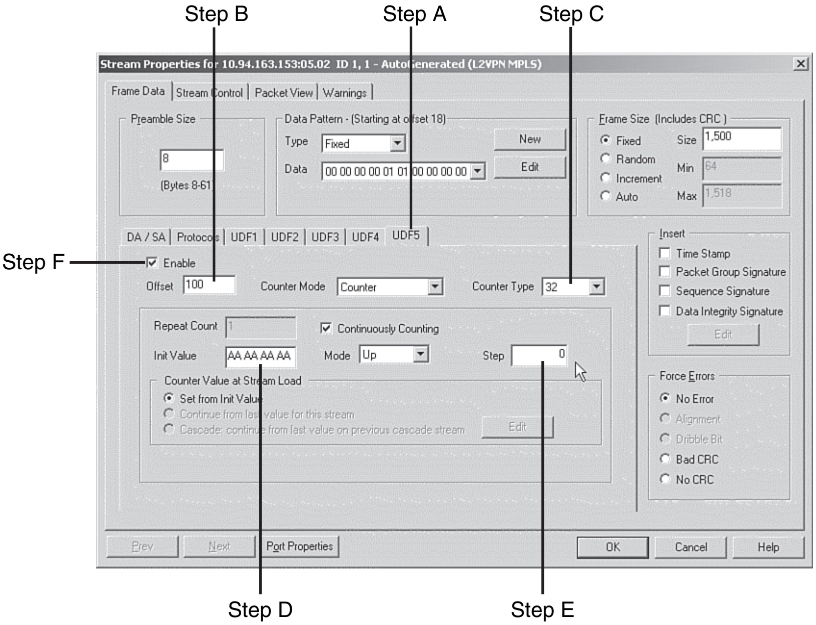
Step C—Select the counter type as 32.

Step D—Configure the 32-bit pattern "AA AA AA AA." This is your signature in the packet.

Step E—Select step size as 0.

Step F—Enable the UDF.

Figure 15-143 *Configure Packet Signatures*



Stream Properties for 10.94.163.153:05.02 ID 1, 1 - AutoGenerated (L2VPN MPLS)

Preamble Size: 8 (Bytes 8-61)

Data Pattern - (Starting at offset 18)
Type: Fixed
Data: 00 00 00 00 01 01 00 00 00 00

Frame Size (Includes CRC)
● Fixed ○ Random ○ Increment ○ Auto
Size: 1,500
Min: 64
Max: 1,518

☑ Enable
Offset: 100
Counter Mode: Counter
Counter Type: 32
Repeat Count: 1
☑ Continuously Counting
Init Value: AA AA AA AA
Mode: Up
Step: 0

Counter Value at Stream Load
● Set from Init Value
○ Continue from last value for this stream
○ Cascade: continue from last value on previous cascade stream

Insert
☐ Time Stamp
☐ Packet Group Signature
☐ Sequence Signature
☐ Data Integrity Signature

Force Errors
● No Error
○ Alignment
○ Dribble Bit
○ Bad CRC
○ No CRC

Step 2 In this step, start the stream created under 5-2 by going to the Transmit bar in the main window, as displayed in Figure 15-144. Use the Transmit bar to

(a) Click the **Start Transmit** button.

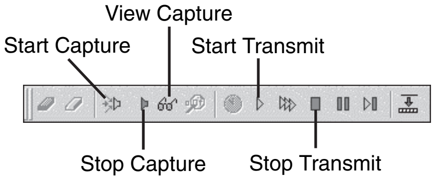
(b) Click the **Start Capture** button. Wait for two to three seconds.

(c) Click the **Stop Transmit** button.

(d) Click the **Stop Capture** button.

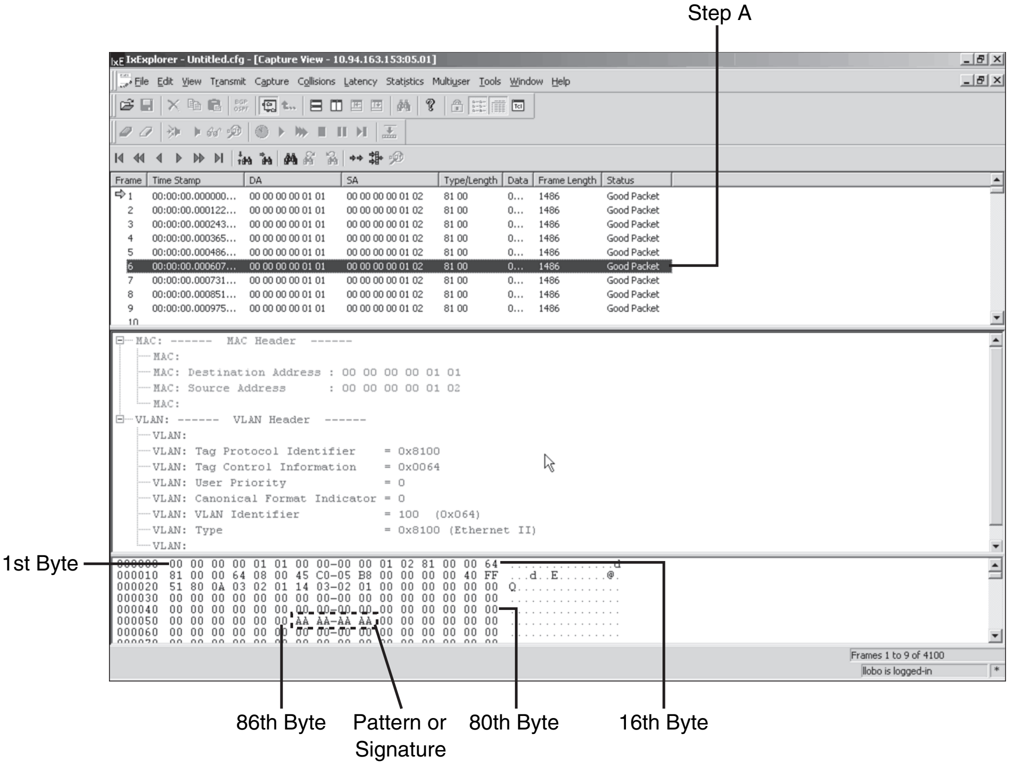
(e) Click the **View Capture** button.

Figure 15-144 *Transmit Bar*



This will take you to the Packet View window shown in Figure 15-145. In the Packet View, look at one of the packets to identify the signature and offset. This is shown in Step A of Figure 15-145, where you click one of the packets and then calculate the offset to the packet signature.

Figure 15-145 *Packet View*


Step A
IxExplorer - Untitled.cfg - [Capture View - 10.94.163.153:05.01]
File Edit View Transmit Capture Collisions Latency Statistics Multiuser Tools Window Help
1st Byte
86th Byte
Pattern or Signature
80th Byte
16th Byte
Frames 1 to 9 of 4100
llobo is logged-in

Frame	Time Stamp	DA	SA	Type/Length	Data	Frame Length	Status
1	00:00:00.000000...	00 00 00 00 01 01	00 00 00 00 01 02	81 00	0...	1486	Good Packet
2	00:00:00.000122...	00 00 00 00 01 01	00 00 00 00 01 02	81 00	0...	1486	Good Packet
3	00:00:00.000243...	00 00 00 00 01 01	00 00 00 00 01 02	81 00	0...	1486	Good Packet
4	00:00:00.000365...	00 00 00 00 01 01	00 00 00 00 01 02	81 00	0...	1486	Good Packet
5	00:00:00.000486...	00 00 00 00 01 01	00 00 00 00 01 02	81 00	0...	1486	Good Packet
6	00:00:00.000607...	00 00 00 00 01 01	00 00 00 00 01 02	81 00	0...	1486	Good Packet
7	00:00:00.000731...	00 00 00 00 01 01	00 00 00 00 01 02	81 00	0...	1486	Good Packet
8	00:00:00.000851...	00 00 00 00 01 01	00 00 00 00 01 02	81 00	0...	1486	Good Packet
9	00:00:00.000975...	00 00 00 00 01 01	00 00 00 00 01 02	81 00	0...	1486	Good Packet
10							

```
MAC: ------  MAC Header  ------
  MAC:
  MAC: Destination Address : 00 00 00 00 01 01
  MAC: Source Address      : 00 00 00 00 01 02
  MAC:
VLAN: ------  VLAN Header  ------
  VLAN:
  VLAN: Tag Protocol Identifier    = 0x8100
  VLAN: Tag Control Information    = 0x0064
  VLAN: User Priority              = 0
  VLAN: Canonical Format Indicator = 0
  VLAN: VLAN Identifier            = 100  (0x064)
  VLAN: Type                       = 0x8100 (Ethernet II)
  VLAN:
```

```
000000 00 00 00 00 01 01 00 00-00 00 01 02 81 00 00 64 ...............d
000010 81 00 00 64 08 00 45 C0-05 B8 00 00 00 00 40 FF ...d..E.......@.
000020 51 80 0A 03 02 01 14 03-02 01 00 00 00 00 00 00 Q...............
000030 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
000040 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
000050 00 00 00 00 00 00 AA AA-AA AA 00 00 00 00 00 00 ................
000060 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
```

Step 3 Follow these steps, as displayed in Figure 15-146:

Step A—Select the **Card 5, Port 1**.

Step B—Double-click **Filter, Statistics, Receive Mode**.

Step C—Select **User Defined Statistics 1**.

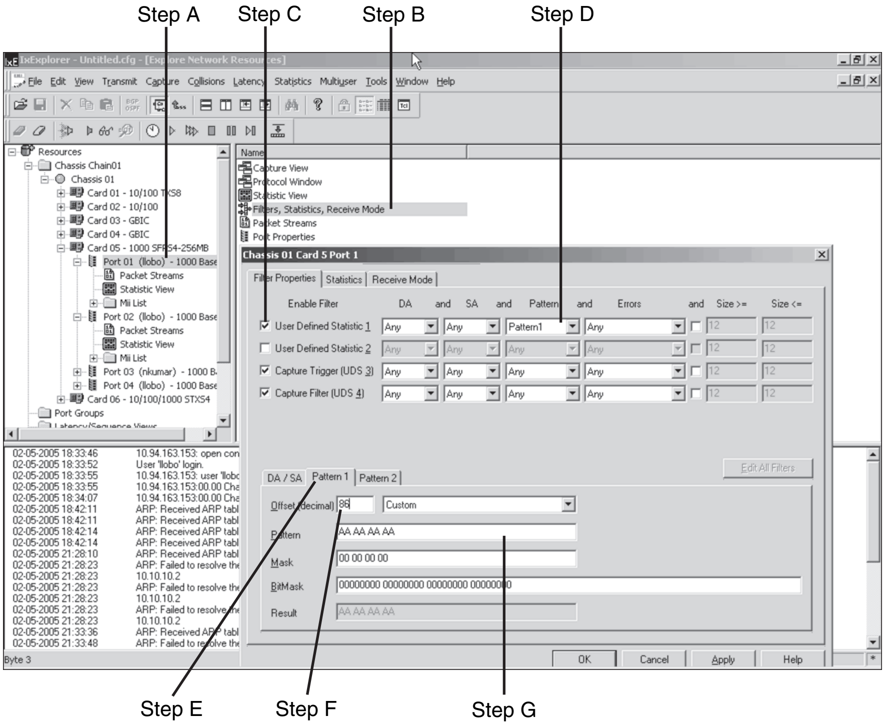
Step D—Select **Pattern1**.

Step E—Select **Pattern 1** tab.

Step F—Configure the offset as 86. This should be calculated as per the packet view shown earlier.

Step G—Configure the pattern. The pattern should match the pattern configured in Step 4.

Figure 15-146 *Defining Filter on Card 5, Port 1*



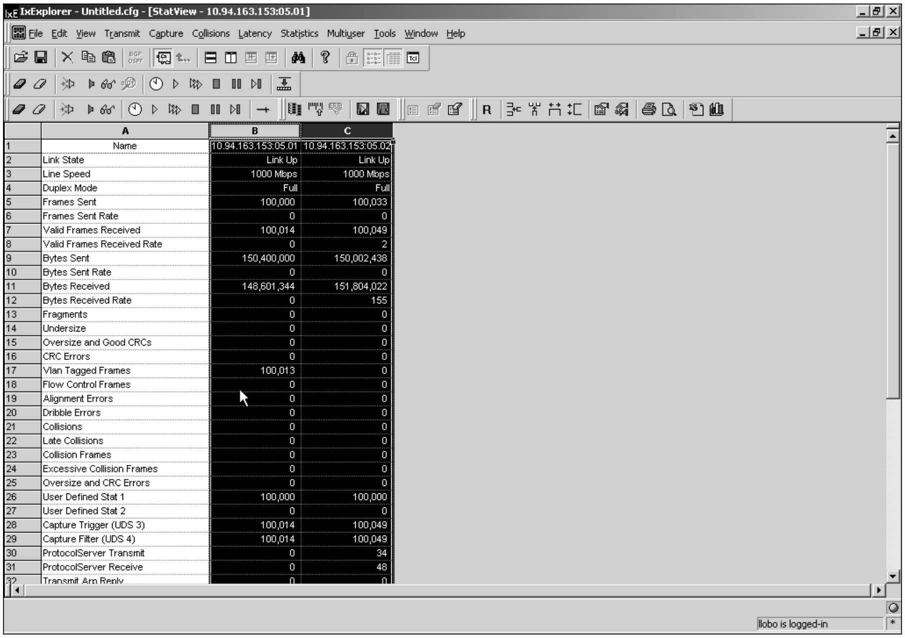
```
02-05-2005 18:33:46   10.94.163.153: open con
02-05-2005 18:33:52   User 'llobo' login.
02-05-2005 18:33:55   10.94.163.153: user 'llobo
02-05-2005 18:33:55   10.94.163.153:00.00 Cha
02-05-2005 18:34:07   10.94.163.153:00.00 Cha
02-05-2005 18:42:11   ARP: Received ARP tabl
02-05-2005 18:42:11   ARP: Received ARP tabl
02-05-2005 18:42:14   ARP: Received ARP tabl
02-05-2005 18:42:14   ARP: Received ARP tabl
02-05-2005 21:28:10   ARP: Received ARP tabl
02-05-2005 21:28:23   ARP: Failed to resolve the
02-05-2005 21:28:23   10.10.10.2
02-05-2005 21:28:23   ARP: Failed to resolve the
02-05-2005 21:28:23   10.10.10.2
02-05-2005 21:28:23   ARP: Failed to resolve the
02-05-2005 21:28:23   10.10.10.2
02-05-2005 21:33:36   ARP: Received ARP tabl
02-05-2005 21:33:48   ARP: Failed to resolve the
```

Enable Filter	DA	and	SA	and	Pattern	and	Errors	and	Size >=	Size <=
☑ User Defined Statistic 1	Any		Any		Pattern1		Any	☐	12	12
☐ User Defined Statistic 2	Any		Any		Any		Any	☐	12	12
☑ Capture Trigger (UDS 3)	Any		Any		Any		Any	☐	12	12
☑ Capture Filter (UDS 4)	Any		Any		Any		Any	☐	12	12

Offset (decimal): 86 Custom
Pattern: AA AA AA AA
Mask: 00 00 00 00
BitMask: 00000000 00000000 00000000 00000000
Result: AA AA AA AA

Step 4 Finally, start the traffic stream by first selecting the stream and then clicking the **Start Transmit** button in the Transmit bar. This will invoke the Statistic View if the Auto-Open on Start-Transmit check box is checked in Tools > Options > Statistic Views. The statistic view for VPLS traffic flowing from 00-00-00-00-01-01 (5-1) to 00-00-00-00-01-02 (5-2) is shown in Figure 15-147.

Figure 15-147 *Statistic View*


IxExplorer - Untitled.cfg - [StatView - 10.94.163.153:05.01]
File Edit View Transmit Capture Collisions Latency Statistics Multiuser Tools Window Help
llobo is logged-in

	A	B	C
1	Name	10.94.163.153:05.01	10.94.163.153:05.02
2	Link State	Link Up	Link Up
3	Line Speed	1000 Mbps	1000 Mbps
4	Duplex Mode	Full	Full
5	Frames Sent	100,000	100,033
6	Frames Sent Rate	0	0
7	Valid Frames Received	100,014	100,049
8	Valid Frames Received Rate	0	2
9	Bytes Sent	150,400,000	150,002,438
10	Bytes Sent Rate	0	0
11	Bytes Received	148,601,344	151,804,022
12	Bytes Received Rate	0	155
13	Fragments	0	0
14	Undersize	0	0
15	Oversize and Good CRCs	0	0
16	CRC Errors	0	0
17	Vlan Tagged Frames	100,013	0
18	Flow Control Frames	0	0
19	Alignment Errors	0	0
20	Dribble Errors	0	0
21	Collisions	0	0
22	Late Collisions	0	0
23	Collision Frames	0	0
24	Excessive Collision Frames	0	0
25	Oversize and CRC Errors	0	0
26	User Defined Stat 1	100,000	100,000
27	User Defined Stat 2	0	0
28	Capture Trigger (UDS 3)	100,014	100,049
29	Capture Filter (UDS 4)	100,014	100,049
30	ProtocolServer Transmit	0	34
31	ProtocolServer Receive	0	48
32	Transmit Arp Reply	0	0

Example 15-22 shows the configuration of the DUT for VPLS testing.

Example 15-22 *DUT Configuration for VPLS*

```
hostname DUT
!
boot system flash disk0:c6k222-pk9sv-mz.122-18.SXD3.bin
!
!
no aaa new-model
ip subnet-zero
!
mpls label protocol ldp
tag-switching tdp discovery directed-hello accept
tag-switching tdp router-id Loopback0 force
mls flow ip destination
mls flow ipx destination
l2 vfi VPLS-A manual
 vpn id 100
 neighbor 10.10.10.102 encapsulation mpls
 neighbor 10.10.10.103 encapsulation mpls
 neighbor 10.10.10.104 encapsulation mpls
!
spanning-tree mode pvst
!
vlan internal allocation policy ascending
vlan dot1q tag native
!
```

continues

Example 15-22 *DUT Configuration for VPLS (Continued)*

```
interface Loopback0
 ip address 10.10.10.101 255.255.255.255
!
interface GE-WAN3/3
 description to ixia 5-2
 ip address 10.10.10.1 255.255.255.252
 negotiation auto
 tag-switching ip
 mls qos trust dscp
!
interface GigabitEthernet5/1
 no ip address
 load-interval 30
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100
 switchport mode trunk
!
interface Vlan100
 no ip address
 no ip igmp snooping
 xconnect vfi VPLS-A
!
router ospf 1
 log-adjacency-changes
 network 10.10.10.0 0.0.0.255 area 0
```

Testing L3 VPN with Smartbits

The section covers

- Topology for L3 VPN testing
- Testing L3 MPLS VPN functionality with SMB6000

Topology for L3 VPN Testing

Topology used in the test setup attempts to emulate the network, as shown in Figure 15-148. A single Cisco router is configured to perform the functions of the Router PE1 in all test cases for L3 VPN. All other associated CE routers and core routers shown in Figure 15-148 are emulated using two test ports on each of the route/traffic generators.

All directly connected CE routers to PE1 in the topology shown in Figure 15-148 are emulated using logical links (sub-interfaces) with a single physical interface connecting to the route/traffic generator. A second link connecting to the PE from the route/traffic generators emulate the MPLS domain (consisting of Routers P1, PE2, PE3, and PE4) with the appropriate emulated PE routers advertising VPNv4 prefixes mapping to the networks to be advertised by Routers CE2, CE4, and CE6. In all route/traffic generators, no emulation of the remote PE-CE routing protocol is performed. However, VPNv4 routes mapping to prefixes to be advertised by the remote CE routers are advertised by their directly connected emulated PE routers; for example, prefixes 192.168.20.0 and 21.0 to be advertised by CE Router CE2 are emulated by advertising the same prefixes as part of VPN1 on PE2 as VPNv4 routes. The physical connectivity to emulate the network shown in Figure 15-148 is depicted in Figure 15-149.

Figure 15-148 *Topology*

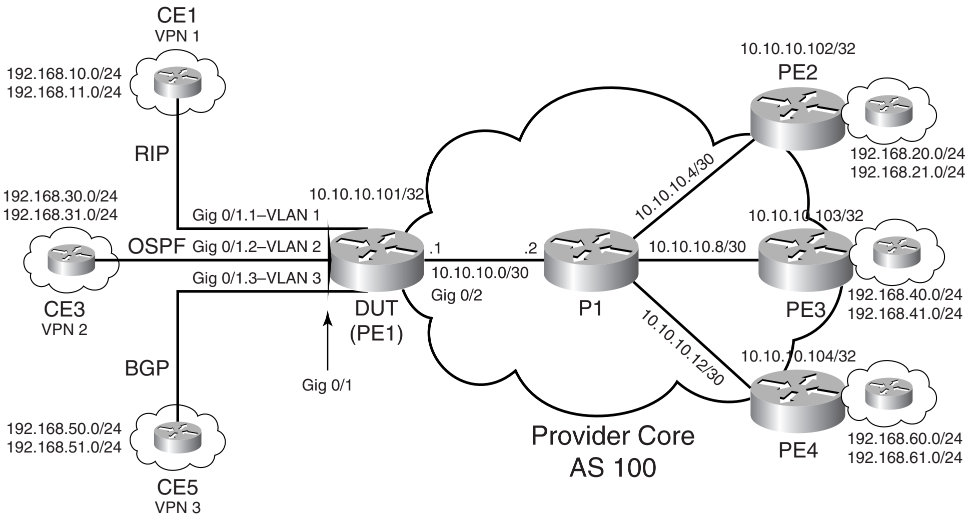
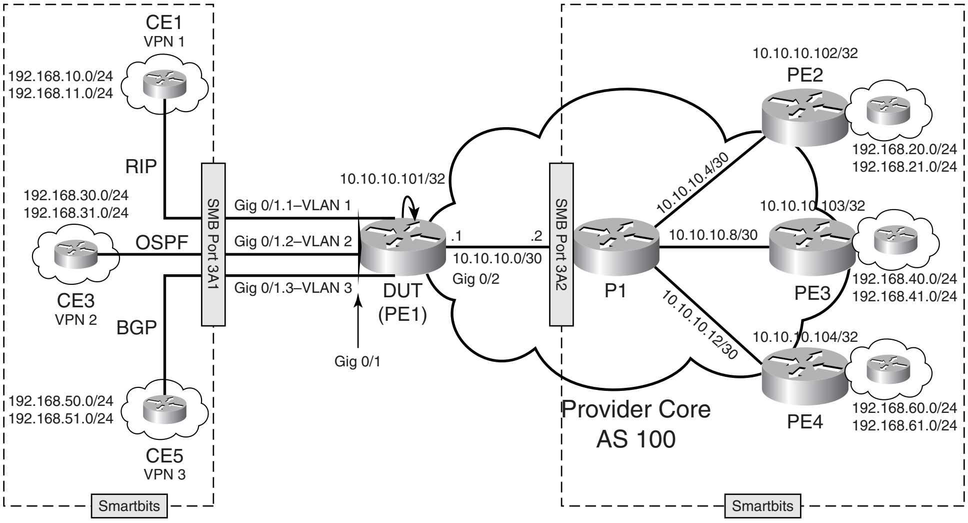


Figure 15-149 *Physical Connectivity*



Testing L3 MPLS VPN Functionality with SMB6000

To test MPLS VPN PE functionality, you will emulate a network, as shown in Figure 15-148, in which the DUT is PE1. The traffic generator and its ports are used to configure and emulate the rest of the network shown in Figure 15-149.

Conditions and Prerequisites

The following outlines the conditions and prerequisites for testing L3 MPLS VPNs with the Smartbits 6000 chassis:

- This test requires two ports on the route/traffic generator: one port to emulate CE connectivity to the DUT and the other port to emulate the MPLS domain, which includes provider core routers and PE routers and remote CE routers belonging to multiple VPNs.
- This test involves the emulation of three CE routers belonging to different VPNs—VPN1 to VPN3—connecting to the DUT using Gigabit Ethernet sub-interfaces. Each VPN generates prefixes, as shown in Figure 15-149.
- RIP PE-CE is implemented between PE1 and CE1 (VPN1), OSPF PE-CE is implemented between PE1 and CE2 (VPN2), and BGP PE-CE is implemented between PE1 and CE3 (VPN3).

Example 15-23 shows the configuration of the DUT used for testing MPLS VPN functionality.

Example 15-23 *DUT Configuration for L3 VPN Test*

```
hostname DUT
!
ip cef
!
ip vrf vpn1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
ip vrf vpn2
 rd 1:2
 route-target export 1:2
 route-target import 1:2
!
ip vrf vpn3
 rd 1:3
 route-target export 1:3
 route-target import 1:3
!
interface GigabitEthernet0/1
 description Connected to traffic generator port 1(emulate local CE connections)
!
interface GigabitEthernet0/1.1
 encapsulation dot1Q 1
```

Example 15-23 *DUT Configuration for L3 VPN Test (Continued)*

```
 ip vrf forwarding vpn1
 ip address 172.16.1.2 255.255.255.0
!
interface GigabitEthernet0/1.2
 encapsulation dot1Q 2
 ip vrf forwarding vpn2
 ip address 172.16.2.2 255.255.255.0
!
interface GigabitEthernet0/1.3
 encapsulation dot1Q 3
 ip vrf forwarding vpn3
 ip address 172.16.3.2 255.255.255.0
!
interface GigabitEthernet0/2
 Description- Connection to Traffic Generator port 2 (emulate-MPLS domain)
 ip address 10.10.10.1 255.255.255.252
 mpls label protocol ldp
 mpls ip
!
router ospf 2 vrf vpn2
 log-adjacency-changes
 redistribute bgp 100 metric 10 subnets
 network 172.16.2.0 0.0.0.255 area 0
!
router ospf 100
 log-adjacency-changes
 network 10.10.10.0 0.0.0.3 area 0
 network 10.10.10.101 0.0.0.0 area 0
!
router rip
 version 2
 !
 address-family ipv4 vrf vpn1
 network 172.16.0.0
 no auto-summary
 version 2
 exit-address-family
 !
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.10.10.102 remote-as 100
 neighbor 10.10.10.102 up lo 0
 neighbor 10.10.10.103 remote-as 100
 neighbor 10.10.10.103 up lo 0
 neighbor 10.10.10.104 remote-as 100
 neighbor 10.10.10.104 up lo 0
 no auto-summary
 !
 address-family vpnv4
 neighbor 10.10.10.102 activate
```

continues

Example 15-23 *DUT Configuration for L3 VPN Test (Continued)*

```
 neighbor 10.10.10.102 send-community extended
 neighbor 10.10.10.103 activate
 neighbor 10.10.10.103 send-community extended
 neighbor 10.10.10.104 activate
 neighbor 10.10.10.104 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf vpn3
 neighbor 172.16.3.1 remote-as 65001
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf vpn2
 redistribute ospf 2 vrf vpn2 metric 10
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf vpn1
 redistribute rip metric 3
 no auto-summary
 no synchronization
 exit-address-family
!
```

Testing MPLS VPN Functionality with Spirent Smartbits 6000

For the first test, use the Spirent Smartbits chassis along with a four-port 10/100/1000 line card to test L3 VPN PE functionality of the DUT. For this test, all configurations for route as well as traffic generation are performed on the tool called the *TeraRoutingTester (TRT).* The version used for all screenshots in this chapter is 4.50. Prior to all the configurations in this chapter, the TRT software has to be installed on a client system that can then be used to remotely configure the Smartbits chassis and cards. This will involve purchasing the appropriate licenses and software followed by installation. Installation procedures can be found online at http://www.spirentcom.com. After installation, verify that the IP address assigned to the Smartbits chassis is reachable from the client system prior to configuration.

Establishing Remote Connectivity to Smartbits Using TRT

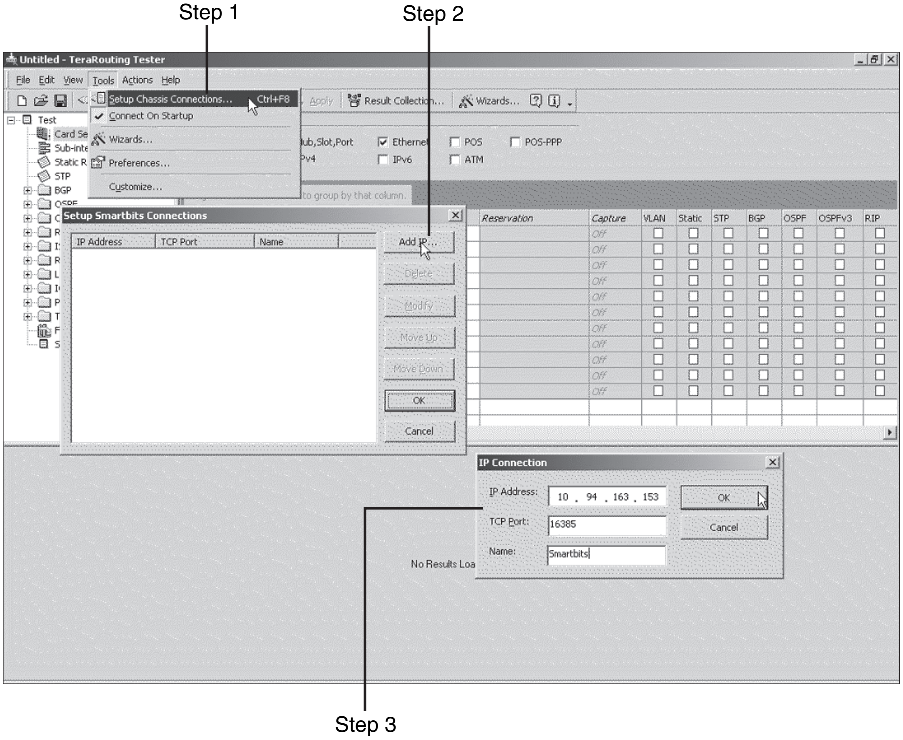
After installation of the TRT software on the client machine, perform the following steps for the addition of a new chassis for connection using the TRT software. The panes as well as the location of the toolbars and naming convention are shown in Figure 15-150:

Step 1 Double-click the **TeraRouting** icon to start the program and click the **Tools** option in the Menu bar.

Step 2 This opens a window, as shown in Figure 15-150. In the new Setup Chassis Connections window, click the **Add IP** button.

Step 3 In the IP Connection window, enter an IP address mapping to the new Smartbits chassis and enter a name for the chassis. Click **OK** to exit out of these two windows into the main TRT application.

Figure 15-150 *Setup New Chassis: Smartbits*



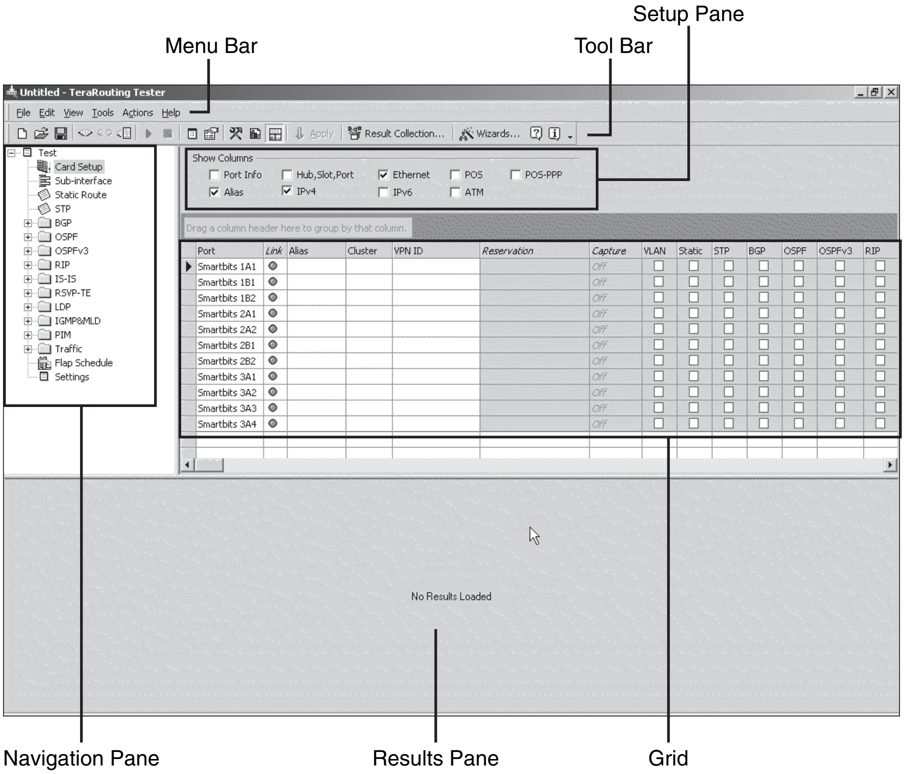
IP Address: 10 . 94 . 163 . 153
TCP Port: 16385
Name: Smartbits

Step 4 Finally, connect to the chassis by clicking **Actions > Connect** in the main toolbar.

Smartbits Port Setup: IP Addressing and Protocol Configuration

The naming convention for the areas used for configuration is shown in Figure 15-151.

Figure 15-151 *Configuration Panes*



Show Columns
☐ Port Info ☐ Hub,Slot,Port ☑ Ethernet ☐ POS ☐ POS-PPP
☑ Alias ☑ IPv4 ☐ IPv6 ☐ ATM

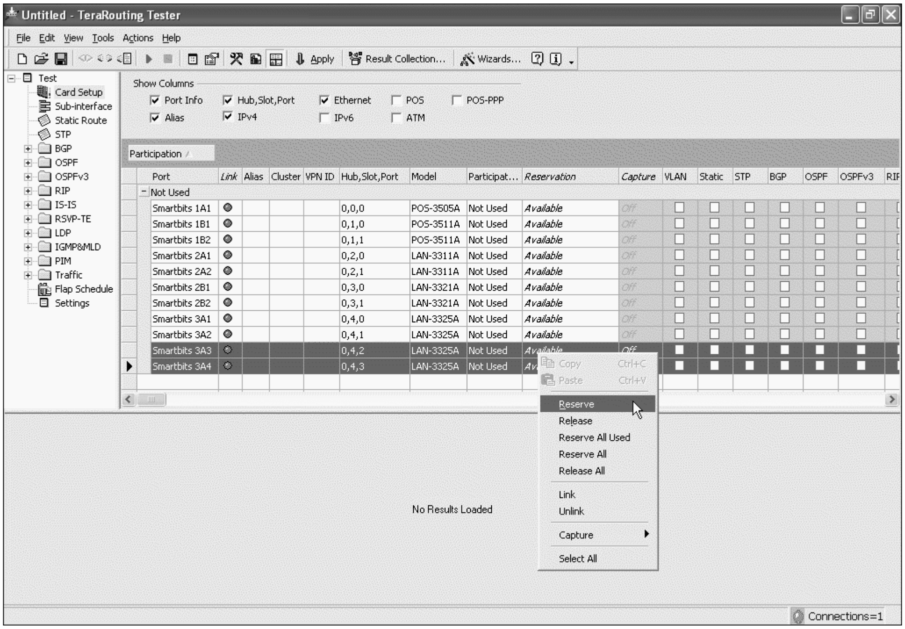
Port	*Link*	Alias	Cluster	VPN ID	*Reservation*	*Capture*	VLAN	Static	STP	BGP	OSPF	OSPFv3	RIP
Smartbits 1A1	●					*Off*	☐	☐	☐	☐	☐	☐	☐
Smartbits 1B1	●					*Off*	☐	☐	☐	☐	☐	☐	☐
Smartbits 1B2	●					*Off*	☐	☐	☐	☐	☐	☐	☐
Smartbits 2A1	●					*Off*	☐	☐	☐	☐	☐	☐	☐
Smartbits 2A2	●					*Off*	☐	☐	☐	☐	☐	☐	☐
Smartbits 2B1	●					*Off*	☐	☐	☐	☐	☐	☐	☐
Smartbits 2B2	●					*Off*	☐	☐	☐	☐	☐	☐	☐
Smartbits 3A1	●					*Off*	☐	☐	☐	☐	☐	☐	☐
Smartbits 3A2	●					*Off*	☐	☐	☐	☐	☐	☐	☐
Smartbits 3A3	●					*Off*	☐	☐	☐	☐	☐	☐	☐
Smartbits 3A4	●					*Off*	☐	☐	☐	☐	☐	☐	☐

Step 1 Prior to any configuration, the appropriate ports used in the test are reserved, as shown in Figure 15-152. Highlight the ports to be used in the test and right-click the reservation column. Select the **Reserve** option. Figure 15-152 shows the port reservation for ports Smartbits 3A1 and Smartbits 3A2.

Step 2 Enable both the ports by highlighting and right-clicking in the grid under the Participation column and selecting the **Xmit and Advertise** option as shown in Figure 15-153. Soon after, click the **Apply** button in the toolbar to enable the respective ports.

Step 3 Enter a name for each of the ports under the Alias section, depending on the function of the port on the traffic generator. Note that the alias functions as a placeholder for the user alone and is not used in any portions of configurations except as a pointer to the port in question.

Figure 15-152 *Port Reservation*



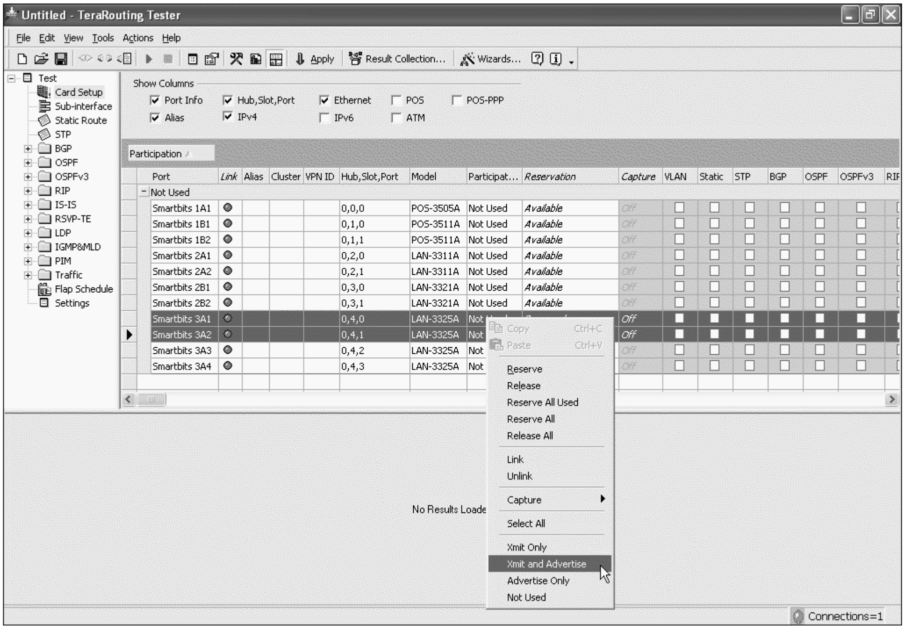
Show Columns

☑ Port Info ☑ Hub,Slot,Port ☑ Ethernet ☐ POS ☐ POS-PPP
☑ Alias ☑ IPv4 ☐ IPv6 ☐ ATM

Not Used

Port	Link	Alias	Cluster	VPN ID	Hub,Slot,Port	Model	Participat...	Reservation	Capture	VLAN	Static	STP	BGP	OSPF	OSPFv3
Smartbits 1A1	●				0,0,0	POS-3505A	Not Used	Available	Off	☐	☐	☐	☐	☐	☐
Smartbits 1B1	●				0,1,0	POS-3511A	Not Used	Available	Off	☐	☐	☐	☐	☐	☐
Smartbits 1B2	●				0,1,1	POS-3511A	Not Used	Available	Off	☐	☐	☐	☐	☐	☐
Smartbits 2A1	●				0,2,0	LAN-3311A	Not Used	Available	Off	☐	☐	☐	☐	☐	☐
Smartbits 2A2	●				0,2,1	LAN-3311A	Not Used	Available	Off	☐	☐	☐	☐	☐	☐
Smartbits 2B1	●				0,3,0	LAN-3321A	Not Used	Available	Off	☐	☐	☐	☐	☐	☐
Smartbits 2B2	●				0,3,1	LAN-3321A	Not Used	Available	Off	☐	☐	☐	☐	☐	☐
Smartbits 3A1	●				0,4,0	LAN-3325A	Not Used	Available	Off	☐	☐	☐	☐	☐	☐
Smartbits 3A2	●				0,4,1	LAN-3325A	Not Used	Available	Off	☐	☐	☐	☐	☐	☐
Smartbits 3A3	●				0,4,2	LAN-3325A	Not Used	Available	Off	☐	☐	☐	☐	☐	☐
Smartbits 3A4	●				0,4,3	LAN-3325A	Not Used	Av		☐	☐	☐	☐	☐	☐

Figure 15-153 *Enabling Ports*



Show Columns

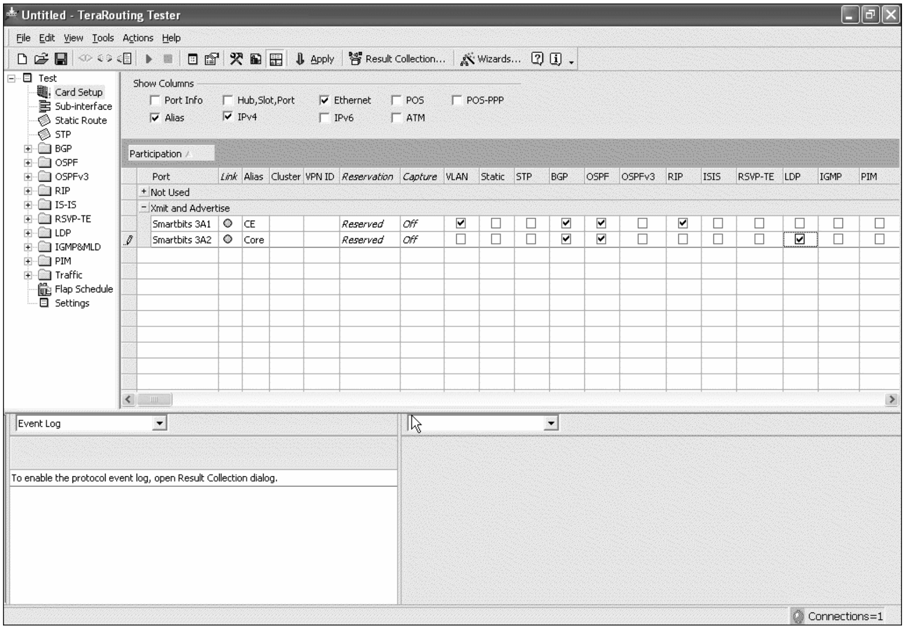
☑ Port Info ☑ Hub,Slot,Port ☑ Ethernet ☐ POS ☐ POS-PPP
☑ Alias ☑ IPv4 ☐ IPv6 ☐ ATM

Not Used

Port	Link	Alias	Cluster	VPN ID	Hub,Slot,Port	Model	Participat...	Reservation	Capture	VLAN	Static	STP	BGP	OSPF	OSPFv3
Smartbits 1A1	●				0,0,0	POS-3505A	Not Used	Available	Off	☐	☐	☐	☐	☐	☐
Smartbits 1B1	●				0,1,0	POS-3511A	Not Used	Available	Off	☐	☐	☐	☐	☐	☐
Smartbits 1B2	●				0,1,1	POS-3511A	Not Used	Available	Off	☐	☐	☐	☐	☐	☐
Smartbits 2A1	●				0,2,0	LAN-3311A	Not Used	Available	Off	☐	☐	☐	☐	☐	☐
Smartbits 2A2	●				0,2,1	LAN-3311A	Not Used	Available	Off	☐	☐	☐	☐	☐	☐
Smartbits 2B1	●				0,3,0	LAN-3321A	Not Used	Available	Off	☐	☐	☐	☐	☐	☐
Smartbits 2B2	●				0,3,1	LAN-3321A	Not Used	Available	Off	☐	☐	☐	☐	☐	☐
Smartbits 3A1	●				0,4,0	LAN-3325A	Not		Off	☐	☐	☐	☐	☐	☐
Smartbits 3A2	●				0,4,1	LAN-3325A	Not		Off	☐	☐	☐	☐	☐	☐
Smartbits 3A3	●				0,4,2	LAN-3325A	Not		Off	☐	☐	☐	☐	☐	☐
Smartbits 3A4	●				0,4,3	LAN-3325A	Not		Off	☐	☐	☐	☐	☐	☐

Step 4 Enable appropriate protocols on the ports on the Smartbits chassis depending on the function of the port. For the CE emulation port, VLAN emulation, BGP, RIP, and OSPF and the PE emulation port are enabled for BGP and OSPF, as well as LDP for label exchange with the port on the DUT. VLANs are enabled on the CE emulation port because the physical Gigabit Ethernet interface is used to emulate three sub-interfaces belonging to three separate VPNs. Figure 15-154 shows the configuration in the setup pane and grid for the Ports 3A1 and 3A2.

Figure 15-154 *Configuring Protocols*



Show Columns
☐ Port Info ☐ Hub,Slot,Port ☑ Ethernet ☐ POS ☐ POS-PPP
☑ Alias ☑ IPv4 ☐ IPv6 ☐ ATM

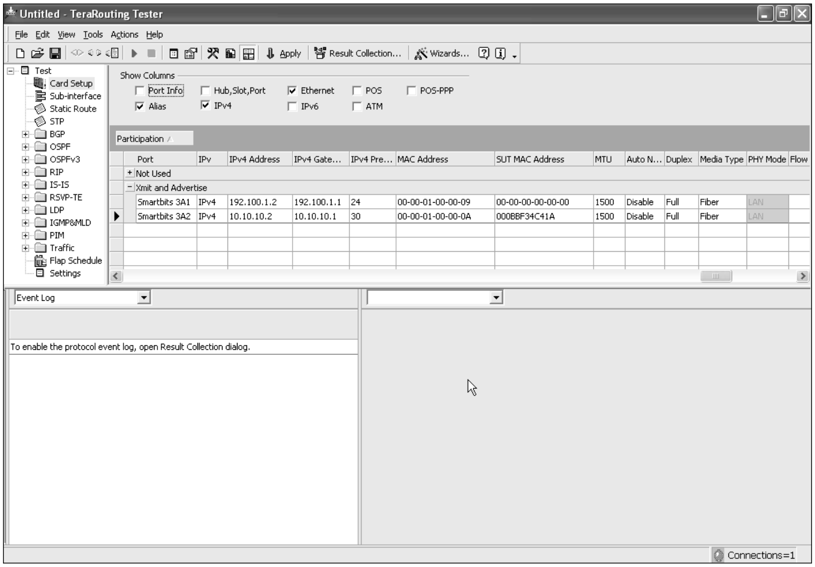
Port	*Link*	Alias	Cluster	VPN ID	*Reservation*	*Capture*	VLAN	Static	STP	BGP	OSPF	OSPFv3	RIP	ISIS	RSVP-TE	LDP	IGMP	PIM
+ Not Used																		
− Xmit and Advertise																		
Smartbits 3A1	○	CE			*Reserved*	*Off*	☑	☐	☐	☑	☑	☐	☑	☐	☐	☐	☐	☐
Smartbits 3A2	○	Core			*Reserved*	*Off*	☐	☐	☐	☑	☑	☐	☐	☐	☐	☑	☐	☐

To enable the protocol event log, open Result Collection dialog.

Step 5 Configure the appropriate IP addresses, as shown in Figure 15-155, for the Smartbits interfaces. Note that because you are configuring three separate interfaces on the CE emulation port on Smartbits, no configuration is required in this step for the CE port. It is recommended to enter the actual interface MAC address, as on the DUT, as the appropriate SUT MAC address. Configuration of the same in the *grid* is shown in Figure 15-155.

Step 6 Click the **Sub-Interface** option on the left-hand pane. There are multiple ways to create sub-interfaces. One way is to right-click the precreated sub-interface and click the **New Subinterface** option. Another method is to right-click the precreated sub-interface and click the **Duplicate** option. In this method, a new window opens where the number of new sub-interfaces can be entered. Use one of the methods to create a total of five sub-interfaces that will map to the five simulated CE Routers CE1 through CE5, as displayed in Figure 15-156.

Figure 15-155 *Configuring IP and MAC Addressing*



Show Columns

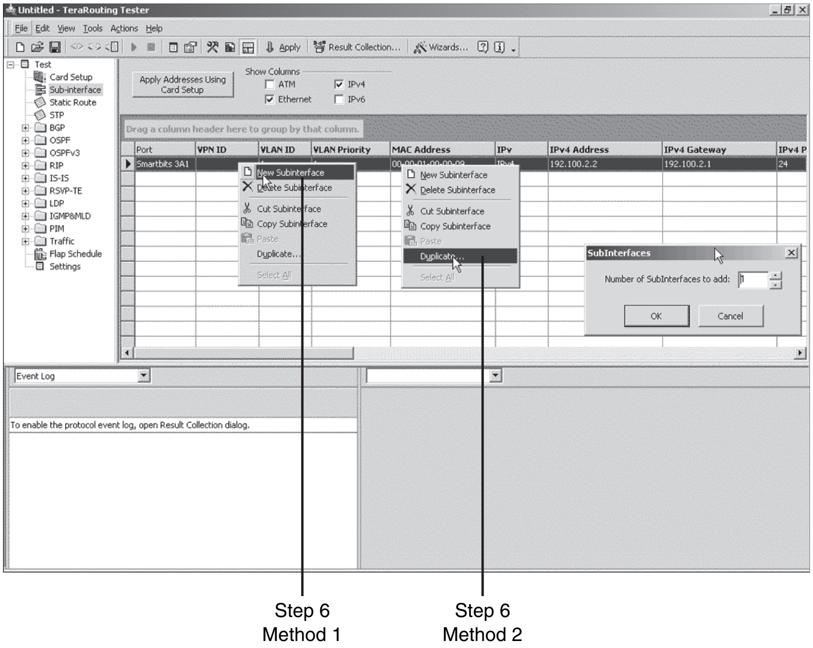
☐ Port Info ☐ Hub,Slot,Port ☑ Ethernet ☐ POS ☐ POS-PPP

☑ Alias ☑ IPv4 ☐ IPv6 ☐ ATM

Port	IPv	IPv4 Address	IPv4 Gate...	IPv4 Pre...	MAC Address	SUT MAC Address	MTU	Auto N...	Duplex	Media Type	PHY Mode	Flow
+ Not Used												
− Xmit and Advertise												
Smartbits 3A1	IPv4	192.100.1.2	192.100.1.1	24	00-00-01-00-00-09	00-00-00-00-00-00	1500	Disable	Full	Fiber	LAN	
Smartbits 3A2	IPv4	10.10.10.2	10.10.10.1	30	00-00-01-00-00-0A	000BBF34C41A	1500	Disable	Full	Fiber	LAN	

To enable the protocol event log, open Result Collection dialog.

Figure 15-156 *Configuring Sub-Interfaces*



Show Columns

☐ ATM ☑ IPv4

☑ Ethernet ☐ IPv6

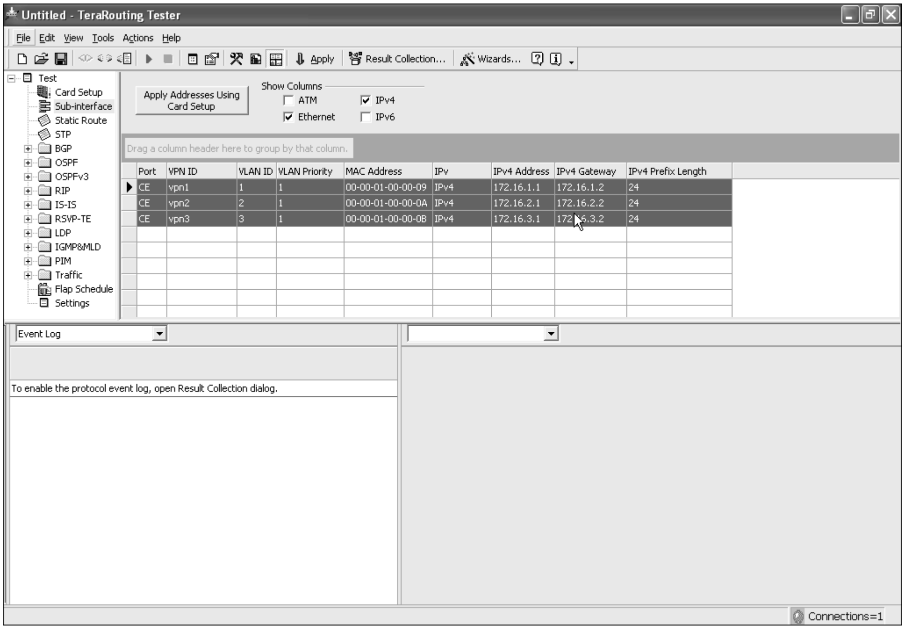
Port	VPN ID	VLAN ID	VLAN Priority	MAC Address	IPv	IPv4 Address	IPv4 Gateway	IPv4 P
Smartbits 3A1				00-00-01-00-00-09	IPv4	192.100.2.2	192.100.2.1	24

Number of SubInterfaces to add: 1

To enable the protocol event log, open Result Collection dialog.

Step 7 Configure the IP addressing for the three VLAN interfaces on the sub-interfaces on the CE emulation port by entering values into the grid, as shown in Figure 15-157.

Figure 15-157 *Configuring Sub-Interfaces—IP Address/VLAN/VPN ID*



Show Columns
☐ ATM ☑ IPv4
☑ Ethernet ☐ IPv6

Port	VPN ID	VLAN ID	VLAN Priority	MAC Address	IPv	IPv4 Address	IPv4 Gateway	IPv4 Prefix Length
CE	vpn1	1	1	00-00-01-00-00-09	IPv4	172.16.1.1	172.16.1.2	24
CE	vpn2	2	1	00-00-01-00-00-0A	IPv4	172.16.2.1	172.16.2.2	24
CE	vpn3	3	1	00-00-01-00-00-0B	IPv4	172.16.3.1	172.16.3.2	24

To enable the protocol event log, open Result Collection dialog.

Smartbits RIP PE-CE Configuration

Step 1 In the following three steps, you configure the CE interfaces for RIP PE-CE routing for VPN1 and VPN2:

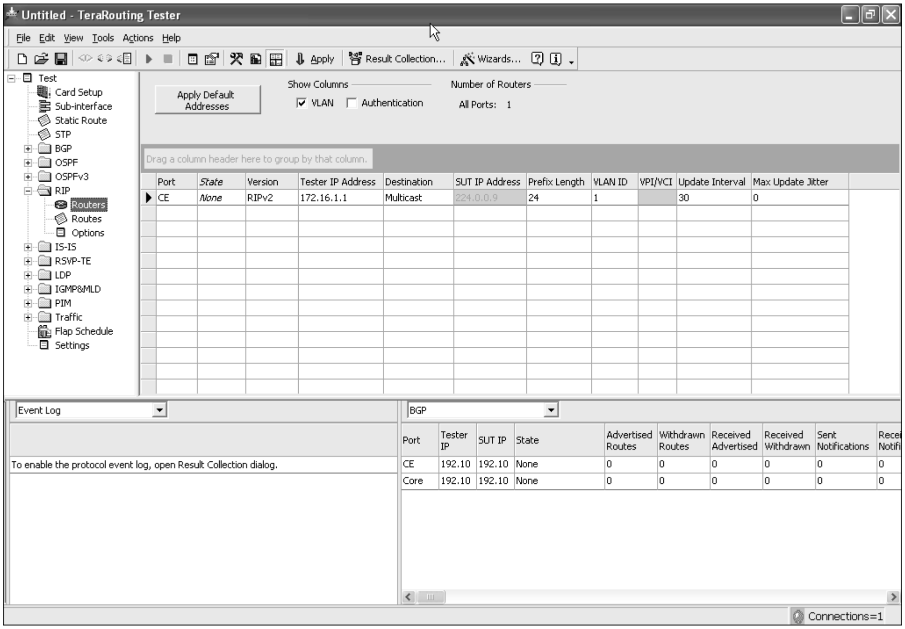
(a) Click and expand the **RIP** tab in the Navigation pane.

(b) Click the **Routers** option under the RIP tab.

(c) Configure the IP addresses appropriately as well as the VLAN ID for the emulated CE for RIP PE-CE routing in the grid, as shown in Figure 15-158.

Step 2 Configure the routes to be generated by the simulated Router CE1 by first clicking the **Routes** option in the Navigation pane. Right-click the first route entry under the RIP router in the grid and select the **New Network** option, as shown in Figure 15-159.

Figure 15-158 *RIP PE-CE—Configure New Routers*



Show Columns

☑ VLAN ☐ Authentication

Number of Routers

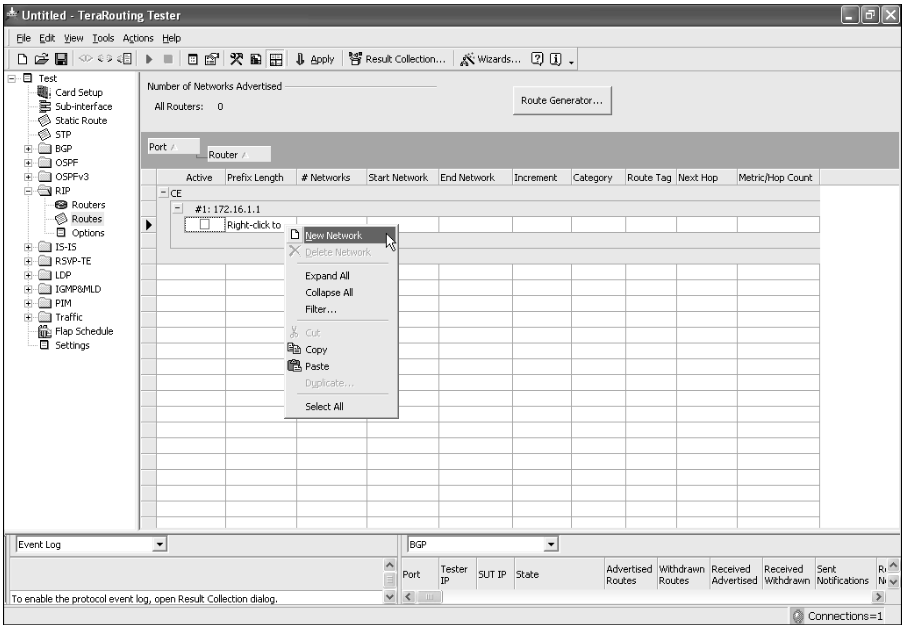
All Ports: 1

Port	State	Version	Tester IP Address	Destination	SUT IP Address	Prefix Length	VLAN ID	VPI/VCI	Update Interval	Max Update Jitter
CE	None	RIPv2	172.16.1.1	Multicast	224.0.0.9	24	1		30	0

To enable the protocol event log, open Result Collection dialog.

Port	Tester IP	SUT IP	State	Advertised Routes	Withdrawn Routes	Received Advertised	Received Withdrawn	Sent Notifications	Recei Notifi
CE	192.10	192.10	None	0	0	0	0	0	0
Core	192.10	192.10	None	0	0	0	0	0	0

Figure 15-159 *RIP PE-CE: Adding Routes-1*



Number of Networks Advertised

All Routers: 0

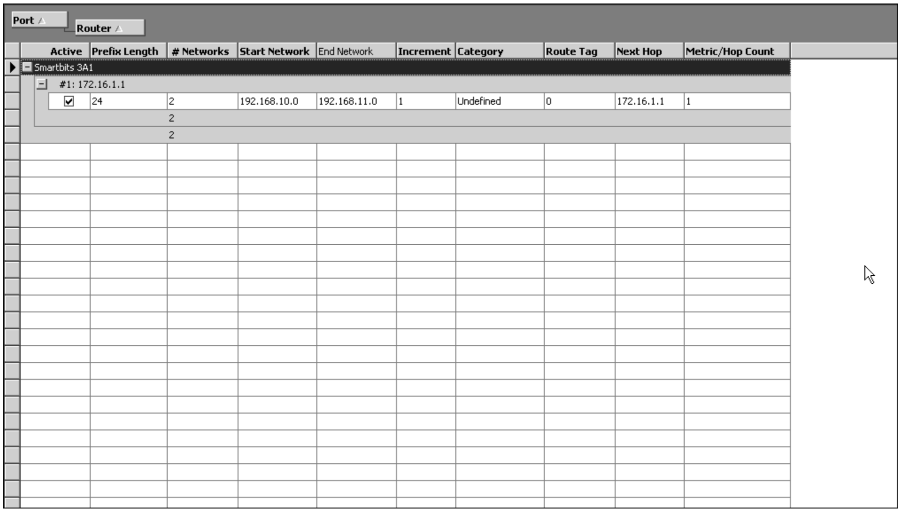
Active	Prefix Length	# Networks	Start Network	End Network	Increment	Category	Route Tag	Next Hop	Metric/Hop Count
CE									
#1: 172.16.1.1									
☐ Right-click to									

To enable the protocol event log, open Result Collection dialog.

Port	Tester IP	SUT IP	State	Advertised Routes	Withdrawn Routes	Received Advertised	Received Withdrawn	Sent Notifications	R N

Step 3 Configure the networks to be advertised by the simulated CE Router CE1 (VPN1) by entering the appropriate values in the grid, as shown in Figure 15-160.

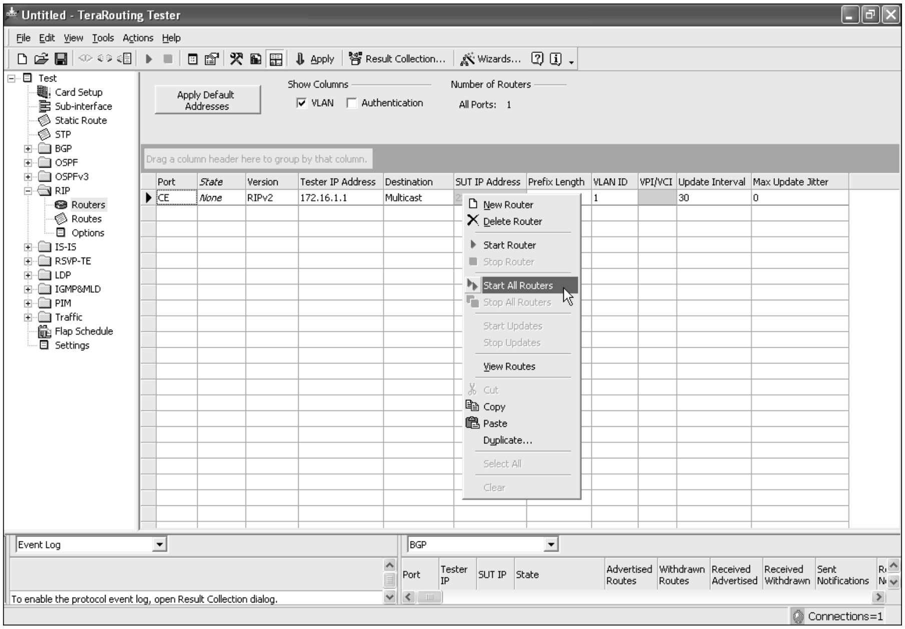
Figure 15-160 *RIP PE-CE: Adding Routes-Grid*



Active	Prefix Length	# Networks	Start Network	End Network	Increment	Category	Route Tag	Next Hop	Metric/Hop Count
Smartbits 3A1									
#1: 172.16.1.1									
☑	24	2	192.168.10.0	192.168.11.0	1	Undefined	0	172.16.1.1	1
		2							
		2							

Step 4 Click the **Routers** tab under RIP in the Navigation pane and right-click and select the option **Start All Routers** in the grid, as illustrated in Figure 15-161.

Figure 15-161 *RIP PE-CE: Start Routers*



Show Columns ☑ VLAN ☐ Authentication

Number of Routers All Ports: 1

Port	State	Version	Tester IP Address	Destination	SUT IP Address	Prefix Length	VLAN ID	VPI/VCI	Update Interval	Max Update Jitter
CE	*None*	RIPv2	172.16.1.1	Multicast			1		30	0

To enable the protocol event log, open Result Collection dialog.

Connections=1

Step 5 The state of the CE routers must change to Open from none, and the DUT must see routes received on the VRF tables for VPN1 as shown by the output of Example 15-24.

Example 15-24 *DUT Verification RIP PE-CE*

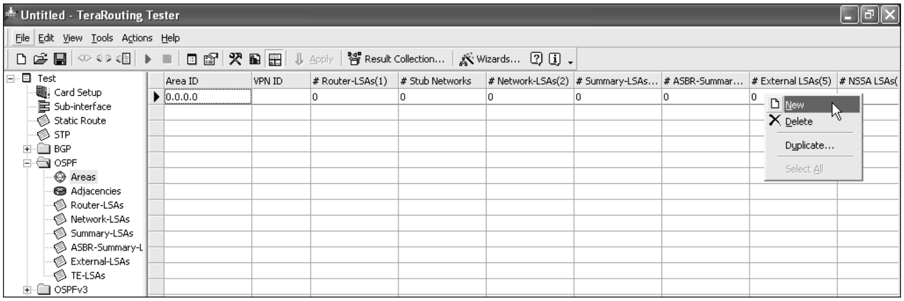
```
DUT#show ip route vrf vpn1 rip
R    192.168.10.0/24 [120/1] via 172.16.1.1, 00:00:28, GigabitEthernet0/1.1
R    192.168.11.0/24 [120/1] via 172.16.1.1, 00:00:28, GigabitEthernet0/1.1
```

Smartbits OSPF PE-CE and OSPF IGP Configuration

This section provides the procedure for the configuration of OSPF for PE-CE sessions as well as OSPF as the IGP in the SP core:

Step 1 Configure OSPF PE-CE connections for VPN VPN2, as displayed in Figure 15-162. Click the **OSPF** tab on the Navigation pane and expand the same and select the **Areas** option. Right-click the default area created in the grid and add one area instance to emulate OSPF PE-CE on VPN2. The default instance will be used later for emulation of OSPF as the IGP in the MPLS core.

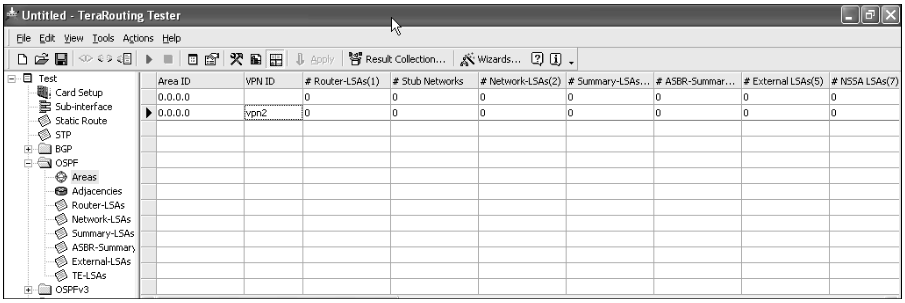
Figure 15-162 *OSPF PE-CE: Add Areas*



Area ID	VPN ID	# Router-LSAs(1)	# Stub Networks	# Network-LSAs(2)	# Summary-LSAs...	# ASBR-Summar...	# External LSAs(5)	# NSSA LSAs(
0.0.0.0		0	0	0	0	0	0	

Step 2 Enter the VPN IDs for the PE-CE instance in the grid and make all areas area 0, as shown in Figure 15-163.

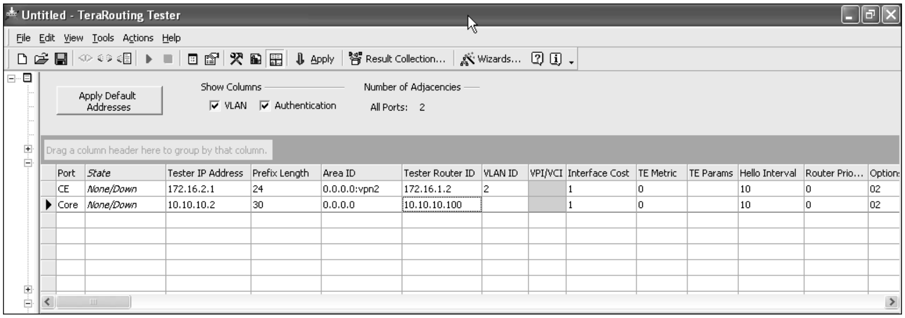
Figure 15-163 *OSPF PE-CE: Add VPN ID for Areas*



Area ID	VPN ID	# Router-LSAs(1)	# Stub Networks	# Network-LSAs(2)	# Summary-LSAs...	# ASBR-Summar...	# External LSAs(5)	# NSSA LSAs(7)
0.0.0.0		0	0	0	0	0	0	0
0.0.0.0	vpn2	0	0	0	0	0	0	0

Step 3 Click the **Adjacencies** option under OSPF in the Navigation pane and configure the parameters of the adjacencies for OSPF PE to CE connections as well as the parameters for OSPF as the IGP for the core. Enter the appropriate addresses for the simulated CE connections (OSPF) as well as the core OSPF instances in the grid, as shown in Figure 15-164. The key parameter in this step is the VLAN ID identifying which sub-interface to run OSPF PE-CE. For the core connections, the tester IP address is configured to be 10.10.10.2/30, as shown in Figure 15-164. The router ID is chosen to be the router ID of the P1 router, which will be the first router interfacing with the DUT in the OSPF domain. Also, select the area ID for the PE-CE connection to be 0.0.0.0:vpn2 from the drop-down menu in the grid under the Area ID column.

Figure 15-164 *OSPF PE-CE: Configure CE and Core Adjacencies*


Untitled - TeraRouting Tester
File Edit View Tools Actions Help
Apply
Result Collection...
Wizards...
Apply Default Addresses
Drag a column header here to group by that column.

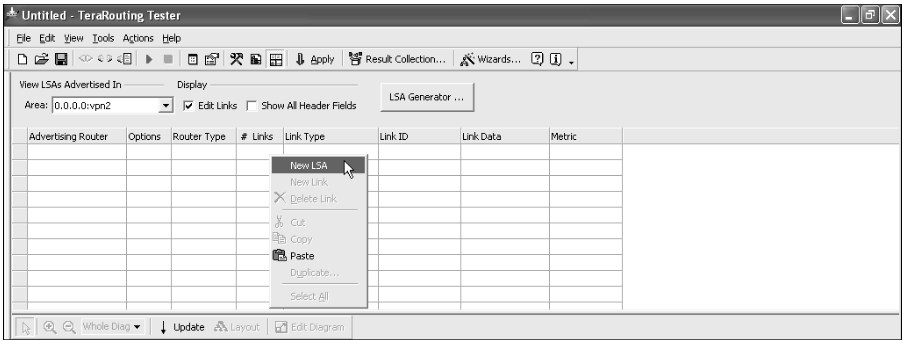
Show Columns: ☑ VLAN ☑ Authentication

Number of Adjacencies: All Ports: 2

Port	*State*	Tester IP Address	Prefix Length	Area ID	Tester Router ID	VLAN ID	VPI/VCI	Interface Cost	TE Metric	TE Params	Hello Interval	Router Prio...	Option:
CE	*None/Down*	172.16.2.1	24	0.0.0.0:vpn2	172.16.1.2	2		1	0		10	0	02
Core	*None/Down*	10.10.10.2	30	0.0.0.0	10.10.10.100			1	0		10	0	02

Step 4 The next step is the addition of the LSAs. For simplicity, we are creating LSAs for networks to be advertised on VPN2 as router LSAs. To create a router LSA, select the **Router LSA** tab from the Navigation pane under OSPF and select the appropriate area for the LSAs in the Setup pane. Figure 15-165 shows the selection of the VPN VPN2 for which we are creating router LSAs. Right-click in the grid and select the option **New LSA**.

Figure 15-165 *OSPF PE-CE: Adding New LSAs*



View LSAs Advertised In: Area: 0.0.0.0:vpn2

Display: ☑ Edit Links ☐ Show All Header Fields

Step 5 Once the new LSA is added, the links that will be advertised as part of the LSA are configured. For VPN2, as shown in Figure 15-166, configure the advertising router to be 172.16.2.1 with two networks advertised.

In Smartbits, the link type defaults to **p2p** (point-to-point) when you add links. However, for the CE simulation, change the link type to **stub** by highlighting all links and right-clicking and selecting the **Stub Network** option.

On the Smartbits TRT tool, when creating LSAs and depending on the link type, the link ID and link data fields entry will vary.

If the link type is **p2p**, the link ID equals the neighbor's router ID, and the link data equals the router's interface IP address, or interface index for unnumbered links.

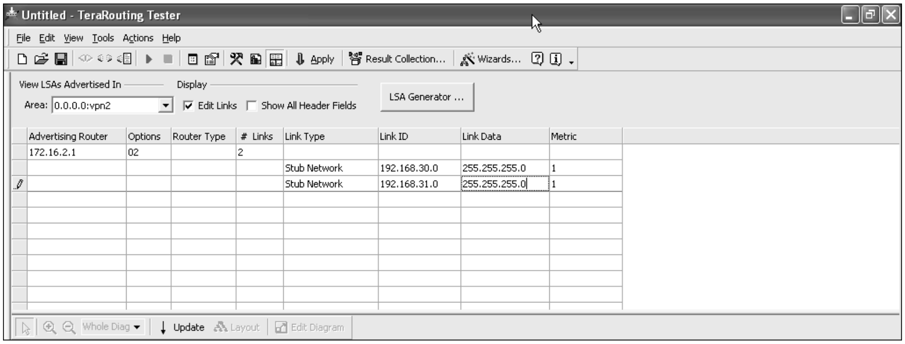
If the link type is **transit network**, the link ID equals the IP address of the designated router's interface and the link data equals the router's interface IP address.

If the link type is **stub network**, the link ID equals the IP network subnet number and link data equals the network's IP address mask.

If the link type is **virtual link**, the link ID equals the neighbor's router ID and the link data equals the router's interface index.

Following these rules, create two stub networks (192.168.30.0-31.0) advertised from router 172.16.2.1, as shown in Figure 15-166.

Figure 15-166 *OSPF PE-CE: LSA Configuration for VPN2*



View LSAs Advertised In

Area: 0.0.0.0:vpn2

Display

☑ Edit Links ☐ Show All Header Fields

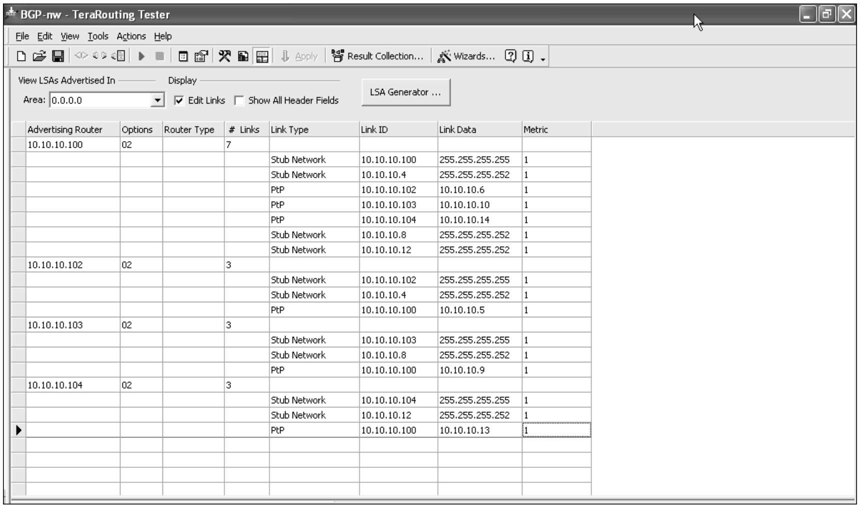
Advertising Router	Options	Router Type	# Links	Link Type	Link ID	Link Data	Metric
172.16.2.1	02		2				
				Stub Network	192.168.30.0	255.255.255.0	1
				Stub Network	192.168.31.0	255.255.255.0	1

Step 6 To configure OSPF as the IGP in the core, you must simulate the provider core routers in the setup P1 as well as the PE Routers PE2, PE3, and PE4, as shown earlier in Figure 15-164.

To emulate the routers in the core, the first step is to select the appropriate area (0.0.0.0) in the Setup pane. You must create one LSA for each

Router P1, PE2, PE3, and PE4. Following the procedures in Step 5, we create appropriate links, as shown in Figure 15-167 in the grid.

Figure 15-167 *OSPF PE-CE: LSA Configuration for MPLS Core*


BGP-nw - TeraRouting Tester
File Edit View Tools Actions Help
Apply
Result Collection...
Wizards...
LSA Generator ...

View LSAs Advertised In

Area: 0.0.0.0

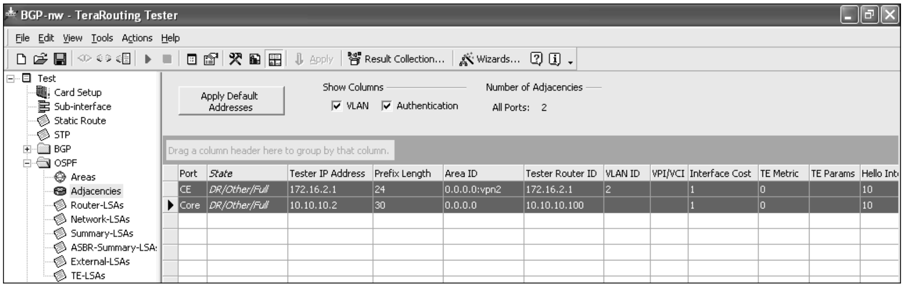
Display

☑ Edit Links ☐ Show All Header Fields

Advertising Router	Options	Router Type	# Links	Link Type	Link ID	Link Data	Metric
10.10.10.100	02		7				
				Stub Network	10.10.10.100	255.255.255.255	1
				Stub Network	10.10.10.4	255.255.255.252	1
				PtP	10.10.10.102	10.10.10.6	1
				PtP	10.10.10.103	10.10.10.10	1
				PtP	10.10.10.104	10.10.10.14	1
				Stub Network	10.10.10.8	255.255.255.252	1
				Stub Network	10.10.10.12	255.255.255.252	1
10.10.10.102	02		3				
				Stub Network	10.10.10.102	255.255.255.255	1
				Stub Network	10.10.10.4	255.255.255.252	1
				PtP	10.10.10.100	10.10.10.5	1
10.10.10.103	02		3				
				Stub Network	10.10.10.103	255.255.255.255	1
				Stub Network	10.10.10.8	255.255.255.252	1
				PtP	10.10.10.100	10.10.10.9	1
10.10.10.104	02		3				
				Stub Network	10.10.10.104	255.255.255.255	1
				Stub Network	10.10.10.12	255.255.255.252	1
				PtP	10.10.10.100	10.10.10.13	1

Step 7 Select the **Adjacencies** tab in the Navigation pane under OSPF, highlight the two rows mapping to the two OSPF adjacencies, and right-click and select the **Start All Routers** option, as performed earlier with the RIP processes in the grid. The State column will now change from None/Down to DR/Other/Full, as shown in Figure 15-168.

Figure 15-168 *OSPF PE-CE: OSPF States*



Show Columns

☑ VLAN ☑ Authentication

Number of Adjacencies

All Ports: 2

Port	State	Tester IP Address	Prefix Length	Area ID	Tester Router ID	VLAN ID	VPI/VCI	Interface Cost	TE Metric	TE Params	Hello Int
CE	*DR/Other/Full*	172.16.2.1	24	0.0.0.0:vpn2	172.16.2.1	2		1	0		10
Core	*DR/Other/Full*	10.10.10.2	30	0.0.0.0	10.10.10.100			1	0		10

Step 8 Verification of the DUT reception of OSPF and operation is shown in Example 15-25.

Example 15-25 *DUT Verification OSPF PE-CE and OSPF IGP*

```
DUT#show ip route vrf vpn2 ospf
Routing Table: vpn2
O    192.168.31.0/24 [110/2] via 172.16.2.1, 00:00:29, GigabitEthernet0/1.2
O    192.168.30.0/24 [110/2] via 172.16.2.1, 00:00:29, GigabitEthernet0/1.2
```

Example 15-25 *DUT Verification OSPF PE-CE and OSPF IGP (Continued)*

```
DUT#sh ip route ospf
     10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O       10.10.10.8/30 [110/3] via 10.10.10.2, 00:00:32, GigabitEthernet0/2
O       10.10.10.4/30 [110/2] via 10.10.10.2, 00:00:32, GigabitEthernet0/2
O       10.10.10.104/32 [110/3] via 10.10.10.2, 00:00:32, GigabitEthernet0/2
O       10.10.10.102/32 [110/3] via 10.10.10.2, 00:00:32, GigabitEthernet0/2
O       10.10.10.103/32 [110/3] via 10.10.10.2, 00:00:32, GigabitEthernet0/2
O       10.10.10.100/32 [110/2] via 10.10.10.2, 00:00:32, GigabitEthernet0/2
```

Smartbits BGP PE-CE and MP-iBGP Configuration

This section provides the procedure for the configuration of BGP for PE-CE sessions as well as MP-iBGP in the emulated SP core:

Step 1 Click the **BGP** tab on the Navigation pane and expand the same. Under BGP, click the **Sessions** option. The grid now identifies the sessions and their configuration from a BGP perspective on the DUT. Four BGP sessions must be created; one with the emulated CE router 172.16.3.1 and one each with the emulated PE routers 10.10.10.102 (PE2), 10.10.10.103 (PE3), and 10.10.10.104 (PE4).

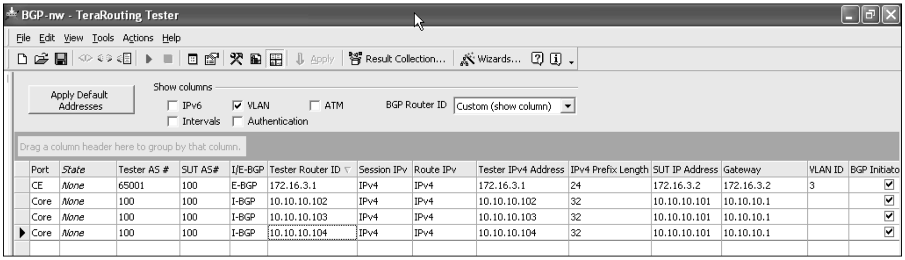
Configurations of the parameters for BGP are entered in the grid, as shown in Figure 15-169, with the following parameters:

CE: Tester AS #, 65001; SUT AS #, 100; Tester IPv4 Address, 172.16.3.1/24; SUT IP Address, 172.16.3.2/24; Gateway, 172.16.3.2 (SUT interface); VLAN ID, 3; Router ID, 172.16.3.1/24

Core Sessions: Tester AS #, 100; SUT AS #, 100; Tester IPv4 Address, 10.10.10.102/32, 10.10.10.103/32, 10.10.10.104/32 (one session per PE router); SUT IP Address, 10.10.10.101; Gateway, 10.10.10.1/30 (SUT interface); Router ID, 10.10.10.102/32 (for PE2), 10.10.10.103/32 (for PE3), and 10.10.10.104/32 (for PE4)

Also, note that you must select the **BGP Router ID** to be of type **Custom** from the Setup pane.

Figure 15-169 *BGP Session Configuration*


BGP-nw - TeraRouting Tester
File Edit View Tools Actions Help
Apply
Result Collection...
Wizards...
Apply Default Addresses
Drag a column header here to group by that column.

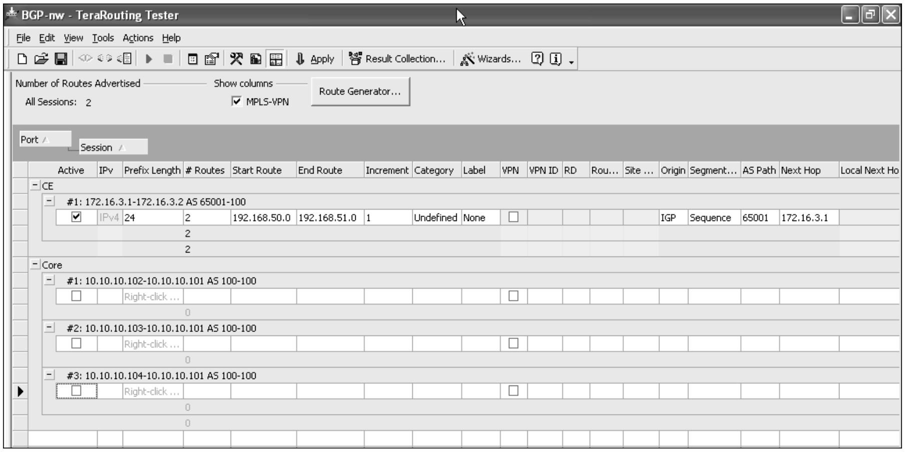
Show columns
☐ IPv6 ☑ VLAN ☐ ATM
☐ Intervals ☐ Authentication

BGP Router ID: Custom (show column)

Port	State	Tester AS #	SUT AS#	I/E-BGP	Tester Router ID	Session IPv	Route IPv	Tester IPv4 Address	IPv4 Prefix Length	SUT IP Address	Gateway	VLAN ID	BGP Initiato
CE	*None*	65001	100	E-BGP	172.16.3.1	IPv4	IPv4	172.16.3.1	24	172.16.3.2	172.16.3.2	3	☑
Core	*None*	100	100	I-BGP	10.10.10.102	IPv4	IPv4	10.10.10.102	32	10.10.10.101	10.10.10.1		☑
Core	*None*	100	100	I-BGP	10.10.10.103	IPv4	IPv4	10.10.10.103	32	10.10.10.101	10.10.10.1		☑
Core	*None*	100	100	I-BGP	10.10.10.104	IPv4	IPv4	10.10.10.104	32	10.10.10.101	10.10.10.1		☑

Step 2 Configure the routes to be generated by each of these sessions by selecting the **Routes** option under **BGP** in Navigation pane. The addition of routes is similar to the addition of routes shown earlier with the RIP protocol in which you right-clicked and selected the option **New Route** in the *grid*. For the CE router, the routes to be generated are 192.168.50 0.0 to 51.0 with the next hop advertised as 172.16.3.1. Figure 15-170 outlines the configuration of CE routes generated by the BGP session with 172.16.3.1.

Figure 15-170 *BGP Route Generation: 172.16.3.1*



Number of Routes Advertised
All Sessions: 2

Show columns
☑ MPLS-VPN

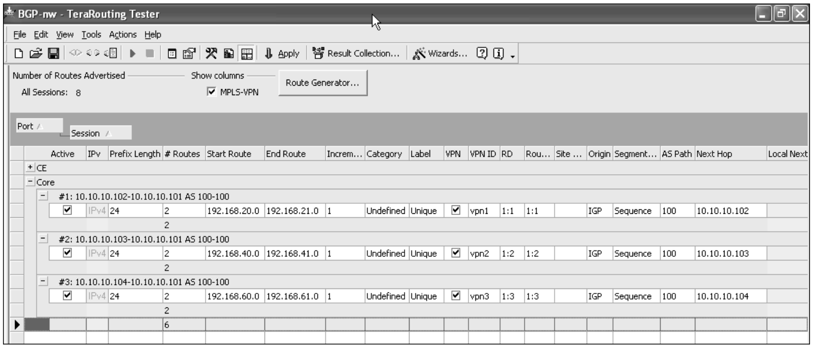
Active	IPv	Prefix Length	# Routes	Start Route	End Route	Increment	Category	Label	VPN	VPN ID	RD	Rou...	Site ...	Origin	Segment...	AS Path	Next Hop	Local Next Ho
CE																		
#1: 172.16.3.1-172.16.3.2 AS 65001-100																		
☑	IPv4	24	2	192.168.50.0	192.168.51.0	1	Undefined	None	☐					IGP	Sequence	65001	172.16.3.1	
			2															
			2															
Core																		
#1: 10.10.10.102-10.10.10.101 AS 100-100																		
☐		Right-click ...							☐									
			0															
#2: 10.10.10.103-10.10.10.101 AS 100-100																		
☐		Right-click ...							☐									
			0															
#3: 10.10.10.104-10.10.10.101 AS 100-100																		
☐		Right-click ...							☐									
			0															
			0															

For the PE router, the routes to be generated are VPNv4 routes mapping to route blocks being generated by remote CE routers. However, care must be taken to add the VPN ID of these route blocks when being advertised by the emulated Router PE2 to map to the correct VRF on the DUT. The configuration is entered as shown in Figure 15-171.

The most important entry to note in Figure 15-171 is the selection of **Unique** under the Label column. This enables association of labels with prefixes and, thus, enables VPNv4 route exchange. Note that without enabling labels, the user is not allowed to configure or enable the VPN parameters.

Step 3 Once the prefixes are configured, select the **Sessions** option under BGP in the Navigation pane. Highlight all sessions in the grid and right-click and select the **Establish Session** option. As illustrated in Figure 15-172, once the session is established, the state of the session changes from Idle to Established.

Figure 15-171 *BGP Route Generation: VPNv4*

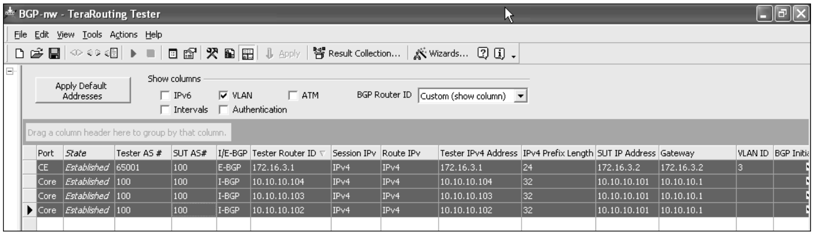


Number of Routes Advertised
All Sessions: 8

Show columns
☑ MPLS-VPN

Active	IPv	Prefix Length	# Routes	Start Route	End Route	Increm...	Category	Label	VPN	VPN ID	RD	Rou...	Site ...	Origin	Segment...	AS Path	Next Hop	Local Next
+ CE																		
− Core																		
− #1: 10.10.10.102-10.10.10.101 AS 100-100																		
☑	IPv4	24	2	192.168.20.0	192.168.21.0	1	Undefined	Unique	☑	vpn1	1:1	1:1		IGP	Sequence	100	10.10.10.102	
			2															
− #2: 10.10.10.103-10.10.10.101 AS 100-100																		
☑	IPv4	24	2	192.168.40.0	192.168.41.0	1	Undefined	Unique	☑	vpn2	1:2	1:2		IGP	Sequence	100	10.10.10.103	
			2															
− #3: 10.10.10.104-10.10.10.101 AS 100-100																		
☑	IPv4	24	2	192.168.60.0	192.168.61.0	1	Undefined	Unique	☑	vpn3	1:3	1:3		IGP	Sequence	100	10.10.10.104	
			2															
			6															

Figure 15-172 *BGP: Establishing Sessions*


BGP-nw - TeraRouting Tester
File Edit View Tools Actions Help
Apply
Result Collection...
Wizards...
Apply Default Addresses
Drag a column header here to group by that column.

Show columns
☐ IPv6 ☑ VLAN ☐ ATM
☐ Intervals ☐ Authentication

BGP Router ID: Custom (show column)

Port	State	Tester AS #	SUT AS#	I/E-BGP	Tester Router ID	Session IPv	Route IPv	Tester IPv4 Address	IPv4 Prefix Length	SUT IP Address	Gateway	VLAN ID	BGP Initia
CE	*Established*	65001	100	E-BGP	172.16.3.1	IPv4	IPv4	172.16.3.1	24	172.16.3.2	172.16.3.2	3	
Core	*Established*	100	100	I-BGP	10.10.10.104	IPv4	IPv4	10.10.10.104	32	10.10.10.101	10.10.10.1		
Core	*Established*	100	100	I-BGP	10.10.10.103	IPv4	IPv4	10.10.10.103	32	10.10.10.101	10.10.10.1		
Core	*Established*	100	100	I-BGP	10.10.10.102	IPv4	IPv4	10.10.10.102	32	10.10.10.101	10.10.10.1		

Step 4 Verify the operation of BGP PE-CE as well as MP-iBGP on the DUT, as shown in Example 15-26.

Example 15-26 *DUT Verification BGP PE-CE and MP-iBGP*

```
DUT#show ip route vrf vpn1 bgp
B    192.168.21.0/24 [200/0] via 10.10.10.102, 00:01:57
B    192.168.20.0/24 [200/0] via 10.10.10.102, 00:01:57
DUT#show ip route vrf vpn2 bgp
B    192.168.40.0/24 [200/0] via 10.10.10.103, 00:02:07
B    192.168.41.0/24 [200/0] via 10.10.10.103, 00:02:07
DUT#show ip route vrf vpn3 bgp
B    192.168.61.0/24 [200/0] via 10.10.10.104, 00:01:56
B    192.168.60.0/24 [200/0] via 10.10.10.104, 00:01:56
B    192.168.51.0/24 [20/0] via 172.16.3.1, 00:02:21
B    192.168.50.0/24 [20/0] via 172.16.3.1, 00:02:21
DUT#
```

Smartbits LDP Configuration

This section provides the procedure for the configuration of LDP with the emulated P router on the Smartbits 6000 chassis:

Step 1 To configure LDP, click the **LDP** option in the Navigation pane and expand the same. In the Sessions grid, configure the following values for the following parameters as shown in Figure 15-173:

Transport Mode: Router ID

Tester IP Address: 10.10.10.2 (interface IP for tester ingress interface)

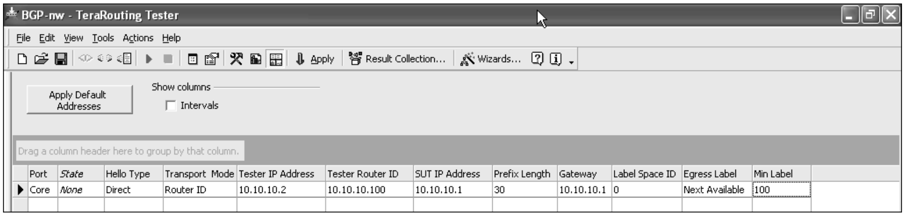
Tester Router ID: 10.10.10.100 (loopback interface of P1 router)

SUT IP Address: 10.10.10.1 (interface IP for SUT egress-core interface)

Egress Label: Next Available

Min Label: 100 (configured to avoid overlapping label spaces—default value is 16)

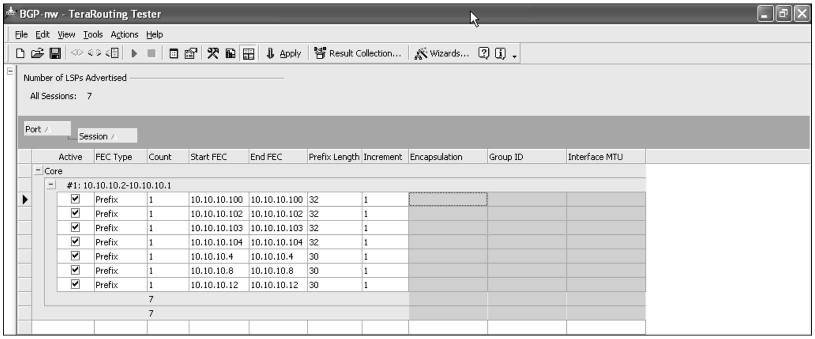
Figure 15-173 *LDP Session Configuration*


BGP-nw - TeraRouting Tester
File Edit View Tools Actions Help
Apply
Result Collection...
Wizards...
Apply Default Addresses
Show columns
☐ Intervals
Drag a column header here to group by that column.

Port	State	Hello Type	Transport Mode	Tester IP Address	Tester Router ID	SUT IP Address	Prefix Length	Gateway	Label Space ID	Egress Label	Min Label
Core	*None*	Direct	Router ID	10.10.10.2	10.10.10.100	10.10.10.1	30	10.10.10.1	0	Next Available	100

Step 2 Once the sessions are configured, you must configure the LSPs that need labels assigned to them. For the core, three LSPs are defined to the following three prefixes as advertised by the IGP: 10.10.10.4/30 (link between PE2 and P1),10.10.10.8/30 (link between PE3 and P1), 10.10.10.12/30 (link between PE4 and P1), 10.10.10.100/32 (P1 loopback) and 10.10.10.102/32 (PE2 loopback), 10.10.10.103/32 (PE3 loopback), and 10.10.10.104/32 (PE4 loopback). To configure the LSPs, select the **LSP** tab under LDP in the Navigation pane. Addition of a new LSP is similar to the addition of a new route block advertisement as mentioned earlier in the RIP and BGP sections. To add a new LSP, right-click in the LSP grid and select the **New LSP** option. For the Start FEC and End FEC values, enter the IP addresses that need an LSP assigned as mentioned earlier and are shown in Figure 15-174.

Figure 15-174 *LDP LSP Configuration*

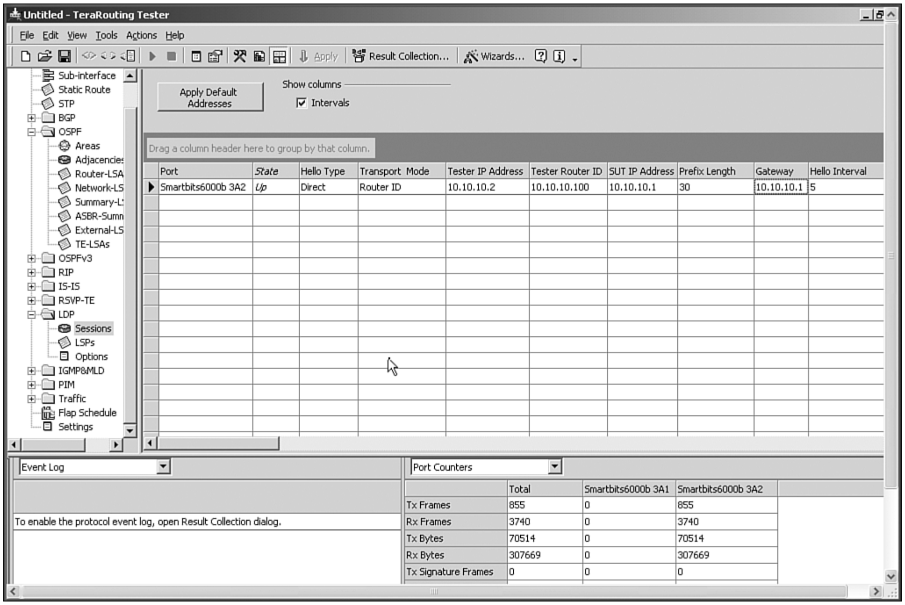

BGP-nw - TeraRouting Tester
File Edit View Tools Actions Help
Apply
Result Collection...
Wizards...
Port
Session

Number of LSPs Advertised
All Sessions: 7

Active	FEC Type	Count	Start FEC	End FEC	Prefix Length	Increment	Encapsulation	Group ID	Interface MTU
Core									
#1: 10.10.10.2-10.10.10.1									
☑	Prefix	1	10.10.10.100	10.10.10.100	32	1			
☑	Prefix	1	10.10.10.102	10.10.10.102	32	1			
☑	Prefix	1	10.10.10.103	10.10.10.103	32	1			
☑	Prefix	1	10.10.10.104	10.10.10.104	32	1			
☑	Prefix	1	10.10.10.4	10.10.10.4	30	1			
☑	Prefix	1	10.10.10.8	10.10.10.8	30	1			
☑	Prefix	1	10.10.10.12	10.10.10.12	30	1			
		7							
		7							

Step 3 The final step in the configuration of LDP is to return to the **Sessions** tab in the Navigation pane. Right-click the session in the Sessions grid and select the **Start Router** option. The state of the session will change from Down to Up, as shown in Figure 15-175.

Figure 15-175 *LDP Session States*



☑ Intervals

Port	State	Hello Type	Transport Mode	Tester IP Address	Tester Router ID	SUT IP Address	Prefix Length	Gateway	Hello Interval
Smartbits6000b 3A2	Up	Direct	Router ID	10.10.10.2	10.10.10.100	10.10.10.1	30	10.10.10.1	5

To enable the protocol event log, open Result Collection dialog.

	Total	Smartbits6000b 3A1	Smartbits6000b 3A2
Tx Frames	855	0	855
Rx Frames	3740	0	3740
Tx Bytes	70514	0	70514
Rx Bytes	307669	0	307669
Tx Signature Frames	0	0	0

Step 4 Verify LDP neighbor relationship and label exchange by performing the appropriate commands on the DUT, as shown in Example 15-27.

Example 15-27 *DUT Verification LDP*

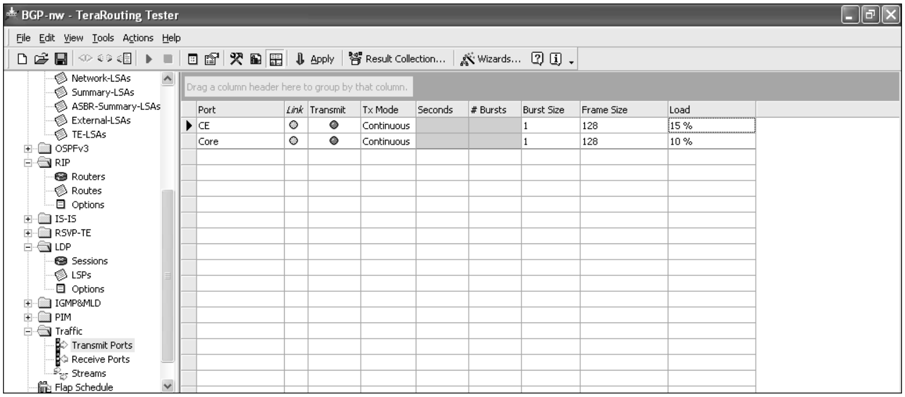
```
DUT#show mpls ldp neighbor
    Peer LDP Ident: 10.10.10.100:0; Local LDP Ident 10.10.10.101:0
        TCP connection: 10.10.10.100.646 - 10.10.10.101.18987
        State: Oper; Msgs sent/rcvd: 12/10; Downstream
        Up time: 00:00:44
        LDP discovery sources:
          GigabitEthernet0/2, Src IP addr: 10.10.10.2
        Addresses bound to peer LDP Ident:
          10.10.10.2
DUT#show mpls ldp bindings neighbor 10.10.10.100
  tib entry: 10.10.10.4/30, rev 102
        remote binding: tsr: 10.10.10.100:0, tag: 104
  tib entry: 10.10.10.8/30, rev 104
        remote binding: tsr: 10.10.10.100:0, tag: 105
  tib entry: 10.10.10.12/30, rev 106
        remote binding: tsr: 10.10.10.100:0, tag: 106
  tib entry: 10.10.10.100/32, rev 108
        remote binding: tsr: 10.10.10.100:0, tag: 100
  tib entry: 10.10.10.102/32, rev 110
        remote binding: tsr: 10.10.10.100:0, tag: 101
  tib entry: 10.10.10.103/32, rev 112
        remote binding: tsr: 10.10.10.100:0, tag: 102
  tib entry: 10.10.10.104/32, rev 114
        remote binding: tsr: 10.10.10.100:0, tag: 103
```

Smartbits MPLS Traffic Generation

In this section, you generate a traffic stream from 192.168.50.0 to 192.168.60.0 via the DUT and verify operation of the same:

Step 1 Select the **Traffic** tab from the Navigation pane and expand the same. Select the **Transmit Ports** tab. In the *grid,* configure the load to be 15 percent on the CE port and 10 percent on the core port for transmit, as illustrated in Figure 15-176.

Figure 15-176 *Configuring Traffic Load*



Port	Link	Transmit	Tx Mode	Seconds	# Bursts	Burst Size	Frame Size	Load
CE	○	●	Continuous			1	128	15 %
Core	○	●	Continuous			1	128	10 %

Step 2 This step is displayed in Figure 15-177:

Step A—Select the **Streams** tab in the Navigation pane.

Step B—In the Setup pane, select the **Traffic Wizard** by clicking on the same.

Step C—Once the Traffic Wizard window opens, select the traffic pattern to be of type **Source > Destination Pairs** and the IP version to be **IPv4**.

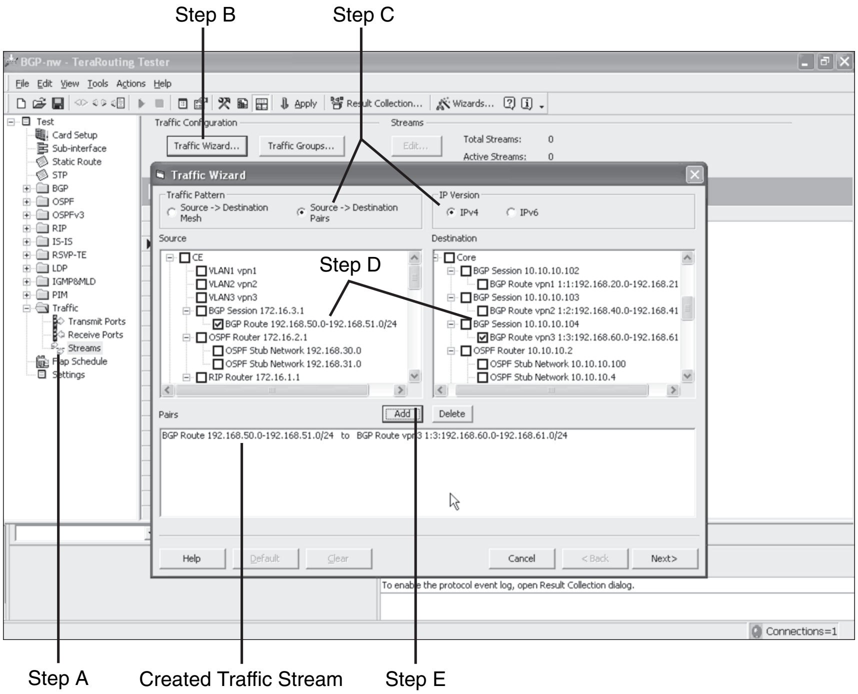
Step D—In the Source window, select the CE prefix 192.168.50.0-51.0 and, in the Destination window, select the core prefix 192.168.60.0-61.0.

Step E—Finally, click the **Add** button in the Traffic Wizard window to add the new traffic stream, as shown in Figure 15-177.

Step 3 Because we want to create bidirectional streams, configure a second stream by repeating Steps 2C through 2E but with the source IP address as 192.168.60.0-61.0 and the destination as 192.168.50.0-51.0, as shown by the highlighted stream in Figure 15-178.

Step 4 Click **Next** followed by **Finish** in the traffic wizard. This creates two streams, as configured in the wizard, to appear in the grid, as shown in Figure 15-179.

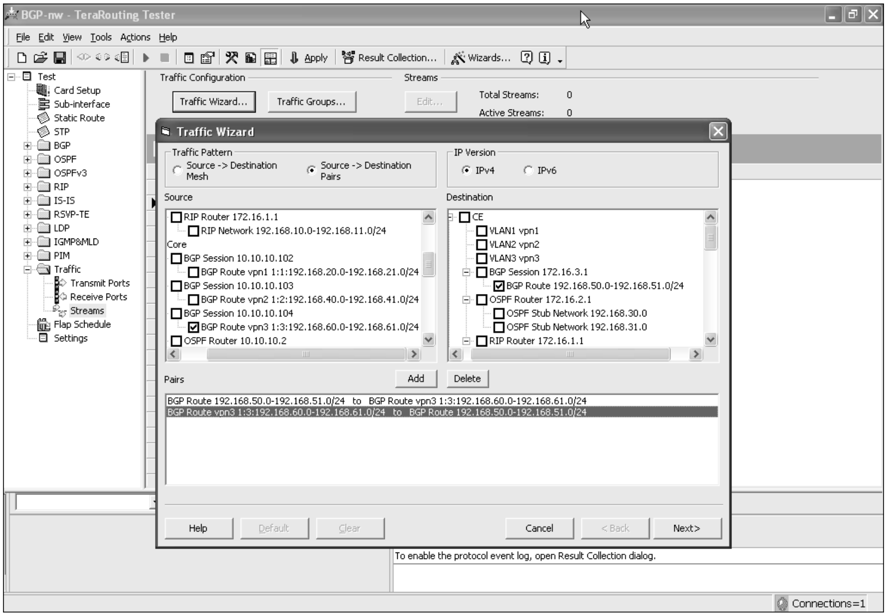
Figure 15-177 *Adding Streams—CE to Core*



BGP Route 192.168.50.0-192.168.51.0/24 to BGP Route vpn3 1:3:192.168.60.0-192.168.61.0/24

To enable the protocol event log, open Result Collection dialog.

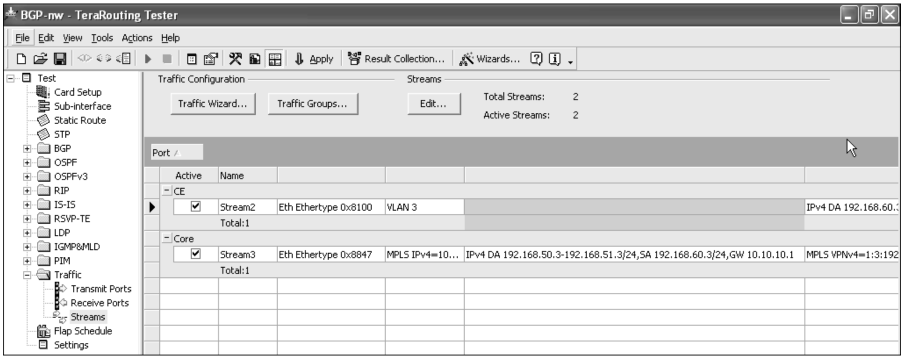
Figure 15-178 *Adding Streams—Core to CE*



BGP Route 192.168.50.0-192.168.51.0/24 to BGP Route vpn3 1:3:192.168.60.0-192.168.61.0/24
BGP Route vpn3 1:3:192.168.60.0-192.168.61.0/24 to BGP Route 192.168.50.0-192.168.51.0/24

To enable the protocol event log, open Result Collection dialog.

Figure 15-179 *Stream Configuration*

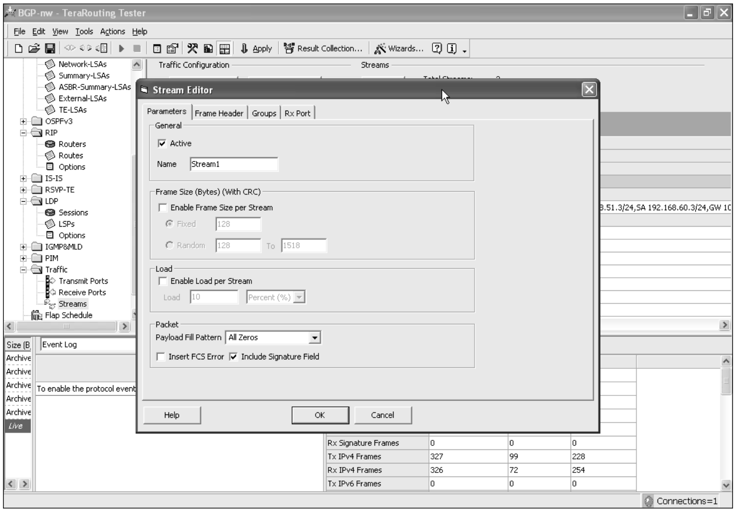


Total Streams: 2
Active Streams: 2

Active	Name				
CE					
☑	Stream2	Eth Ethertype 0x8100	VLAN 3		IPv4 DA 192.168.60.:
	Total:1				
Core					
☑	Stream3	Eth Ethertype 0x8847	MPLS IPv4=10...	IPv4 DA 192.168.50.3-192.168.51.3/24,SA 192.168.60.3/24,GW 10.10.10.1	MPLS VPNv4=1:3:192
	Total:1				

Step 5 Configure signatures for each of the streams by double-clicking the streams in the grid to open the Stream Editor window. Select the **Parameters** tab and select the **Include Signature Field** option, as shown in Figure 15-180, and click **OK**.

Figure 15-180 *Configuring Signatures for Streams*



☑ Active
Name Stream1

☐ Enable Frame Size per Stream
● Fixed 128
○ Random 128 To 1518

☐ Enable Load per Stream
Load 10 Percent (%)

Payload Fill Pattern All Zeros
☐ Insert FCS Error ☑ Include Signature Field

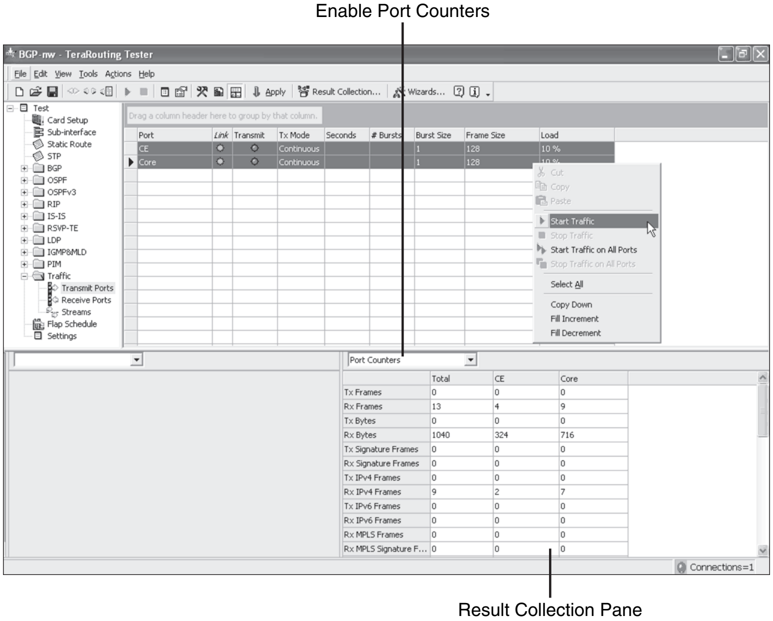
To enable the protocol event

Rx Signature Frames	0	0	0
Tx IPv4 Frames	327	99	228
Rx IPv4 Frames	326	72	254
Tx IPv6 Frames	0	0	0

Step 6 Go back to the **Transmit** tab in the Navigation pane. Prior to traffic generation, select **Port Counters** from the Result Collection drop-down menu, as shown in Figure 15-181. Once this is selected, highlight both ports in the grid and right-click and select the **Start Traffic** option.

Step 7 Once the streams have started, verify operation by verifying that the Tx signature frames from the CE equal the Rx signature frames on the core, and the Tx signature frames on the core equal the Rx signature frames on the CE after stopping the streams, as shown in Figure 15-182.

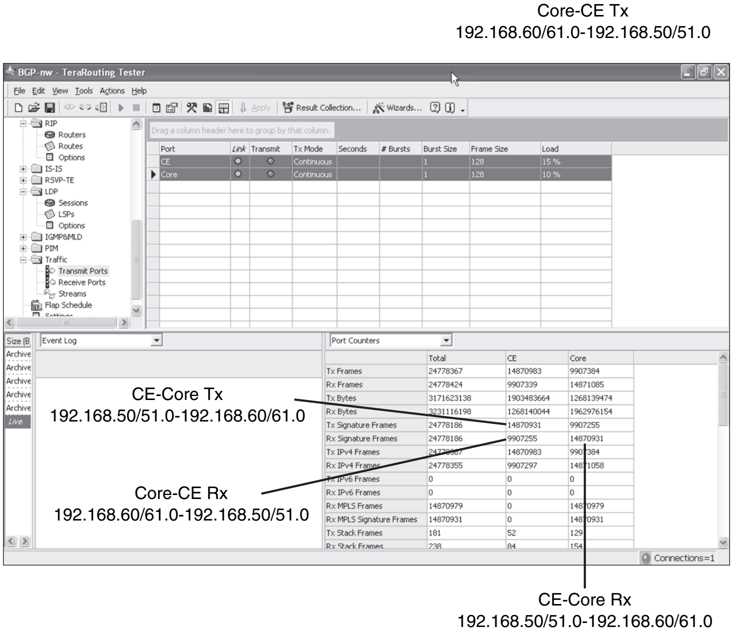
Figure 15-181 *Enabling Port Counters and Traffic Generation*



Port	Link	Transmit	Tx Mode	Seconds	# Bursts	Burst Size	Frame Size	Load
CE	○	○	Continuous			1	128	10 %
Core	○	○	Continuous			1	128	10 %

	Total	CE	Core
Tx Frames	0	0	0
Rx Frames	13	4	9
Tx Bytes	0	0	0
Rx Bytes	1040	324	716
Tx Signature Frames	0	0	0
Rx Signature Frames	0	0	0
Tx IPv4 Frames	0	0	0
Rx IPv4 Frames	9	2	7
Tx IPv6 Frames	0	0	0
Rx IPv6 Frames	0	0	0
Rx MPLS Frames	0	0	0
Rx MPLS Signature F...	0	0	0

Figure 15-182 *Verification of Traffic Generation*



Port	Link	Transmit	Tx Mode	Seconds	# Bursts	Burst Size	Frame Size	Load
CE	○	○	Continuous			1	128	15 %
Core	○	○	Continuous			1	128	10 %

	Total	CE	Core
Tx Frames	24778367	14870983	9907384
Rx Frames	24778424	9907339	14871085
Tx Bytes	3171623138	1903483664	1268139474
Rx Bytes	3231116198	1268140044	1962976154
Tx Signature Frames	24778186	14870931	9907255
Rx Signature Frames	24778186	9907255	14870931
Tx IPv4 Frames	24778367	14870983	9907384
Rx IPv4 Frames	24778355	9907297	14871058
Tx IPv6 Frames	0	0	0
Rx IPv6 Frames	0	0	0
Rx MPLS Frames	14870979	0	14870979
Rx MPLS Signature Frames	14870931	0	14870931
Tx Stack Frames	181	52	129
Rx Stack Frames	238	84	154

The main reason for the addition of signatures is to avoid the addition of control plane traffic not pertaining to the stream to be added into the Rx.

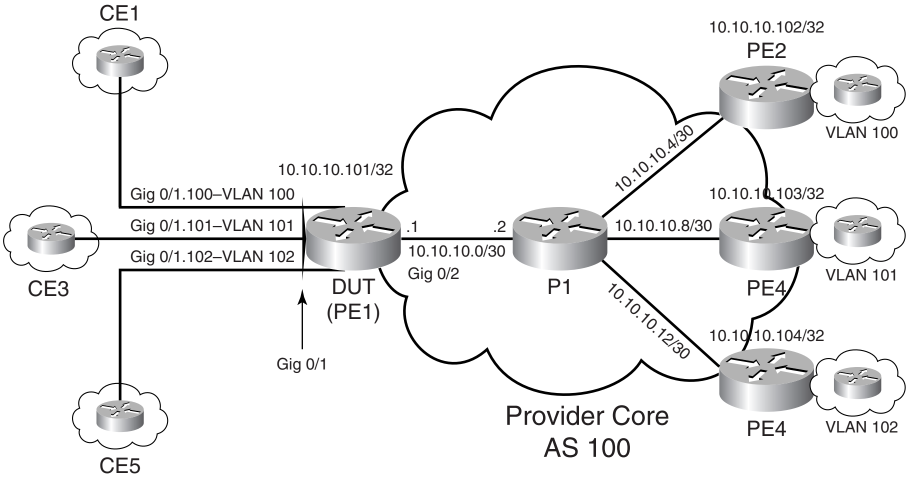
Testing L2 VPN with Smartbits

This section deals with the configuration of L2 VPNs in conjunction with the Smartbits 6000 chassis and TRT software. A single DUT and two Smartbits ports are used to emulate the CE connections and core connections.

Topology for L2 VPN Testing

The topology used in the test setup attempts to emulate the network, as shown in Figure 15-183. A single Cisco router is configured to perform the functions of the Router PE1 in all test cases for L2 VPN. All other associated CE routers and core routers shown in Figure 15-183 are emulated using two test ports on each of the route/traffic generators.

Figure 15-183 *Topology for L2 VPN Testing*

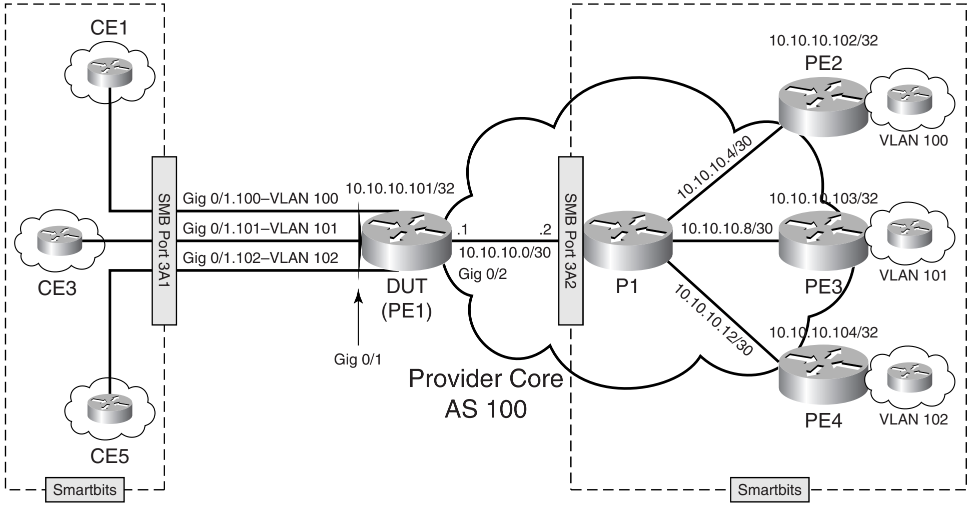


All directly connected CE routers to PE1 in the topology shown in Figure 15-183 are emulated using logical links (sub-interfaces) with a single physical interface connecting to the route/traffic generator. A second link connecting to the PE from the route/traffic generators is used to emulate the MPLS domain (consisting of Routers P1, PE2, PE3, and PE4) with the appropriate emulated PE routers advertising VC prefixes mapping to the networks to be advertised by Routers CE2, CE4, and CE6. In all route/traffic generators, no emulation of the remote PE-CE routing protocol is performed. The physical connectivity to emulate the network shown in Figure 15-183 is depicted in Figure 15-184.

Testing L2 MPLS VPN

To test MPLS VPN PE functionality, you emulate a network, as shown in Figure 15-183, in which the DUT is PE1. The traffic generator and its ports are used to configure and emulate the rest of the network shown in Figure 15-184.

Figure 15-184 *Physical Connectivity*



Conditions and Prerequisites

The following outlines the conditions and prerequisites for the implementation of the topology shown in Figure 15-184:

- This test will require two ports on the route/traffic generator: one port to emulate CE connectivity to the DUT and the other port emulating the MPLS domain, which includes provider core routers and PE routers and remote CE routers belonging to multiple VPNs.
- This test involves the emulation of three CE routers belonging to different L2 VPNs on three different VLANs—100, 101, and 102—connecting to the DUT using Gigabit Ethernet sub-interfaces.

Example 15-28 shows the configuration of the DUT used for testing MPLS VPN functionality.

Example 15-28 *DUT Configuration for L2 VPN Test*

```
hostname DUT
!
ip cef
!
interface Loopback0
 ip address 10.10.10.101 255.255.255.255
 no ip directed-broadcast
!
interface GigabitEthernet0/1
 description Connected to traffic generator port 1(emulate local CE connections)
 no ip address
 no ip directed-broadcast
!
```

continues

Example 15-28 *DUT Configuration for L2 VPN Test (Continued)*

```
interface GigabitEthernet0/1.100
 encapsulation dot1Q 100
 no cdp enable
 xconnect 10.10.10.102 100 encapsulation mpls
!
interface GigabitEthernet0/1.101
 encapsulation dot1Q 101
 no cdp enable
 xconnect 10.10.10.103 101 encapsulation mpls
!
interface GigabitEthernet0/1.102
 encapsulation dot1Q 102
 no cdp enable
 xconnect 10.10.10.104 102 encapsulation mpls
!
interface GigabitEthernet0/2
 ip address 10.10.10.1 255.255.255.252
 mpls label protocol ldp
 tag-switching ip
!
router ospf 100
 log-adjacency-changes
 network 10.10.10.0 0.0.0.3 area 0
 network 10.10.10.101 0.0.0.0 area 0
```

Testing L2 VPN Functionality with Spirent Smartbits 6000

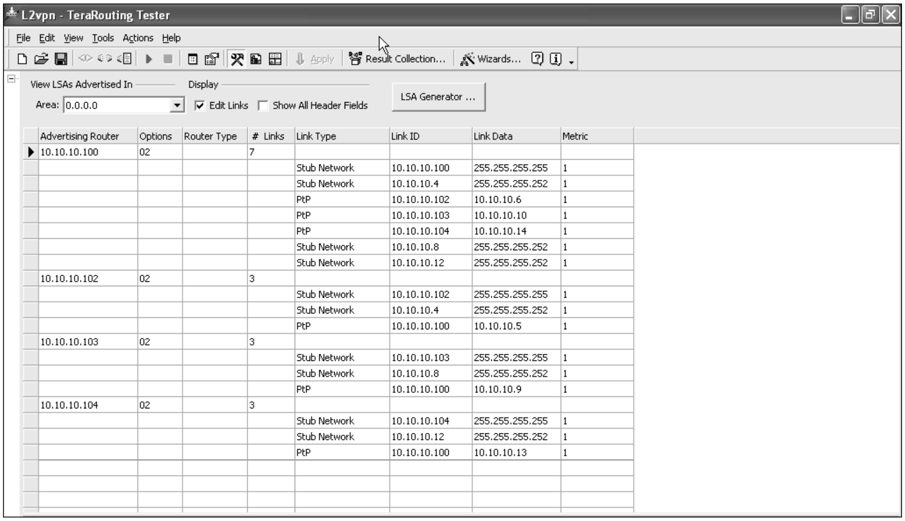
For this test, you use the Spirent Smartbits chassis along with a four-port 10/100/1000 line card to test L2 VPN PE functionality of the DUT. For this test, all configurations for route as well as traffic generation are performed on the TRT. The version used for all screenshots in this chapter is 4.50. Prior to all the configurations in this chapter, the TRT software has to be installed on a client system that can then be used to remotely configure the Smartbits chassis and cards. This requires purchasing the appropriate licenses and software followed by installation. Installation procedures can be found online at http://www.spirentcom.com. After installation, verify that the IP address assigned to the Smartbits chassis is reachable from the client system prior to configuration.

Prior to L2 VPN configuration on the Spirent, you must establish remote connectivity to the Smartbits chassis, which is performed as explained in configuring L3 VPN with Smartbits section. Upon completion, the following steps are implemented on the Smartbits chassis for the configuration and implementation of L2 VPN. It is assumed that prior to the following configuration, the IP addressing and MAC addressing have been performed on the appropriate ports to the requirements as outlined in Figure 15-183. It is important to implement the configuration of sub-interfaces on the CE emulation port with VLAN enabled (VLAN 100, 101, and 102) and the core emulation port must have OSPF and LDP enabled (OSPF for IGP and LDP for label exchange and MPLS operation).

Configuring OSPF as IGP for L2 VPN

The configuration of OSPF as the IGP for implementation and verification of L2 VPN functionality is similar to the emulation of the network when implementing L3 VPN. The configuration consists of defining adjacency between the DUT and the router 10.10.10.2 (P1) where the router 10.10.10.2 with router ID 10.10.10.100 generates LSAs that identify the topology of the core network as advertised by OSPF to the DUT. Figure 15-185 shows the configuration of router LSAs for the implementation of L2 VPN in the core using OSPF. The configuration is the same as shown for the core port in the earlier section for implementing L3 VPN.

Figure 15-185 *L2 VPN OSPF—IGP LSA Configuration*



View LSAs Advertised In

Area: 0.0.0.0

Display

☑ Edit Links ☐ Show All Header Fields

Advertising Router	Options	Router Type	# Links	Link Type	Link ID	Link Data	Metric
10.10.10.100	02		7				
				Stub Network	10.10.10.100	255.255.255.255	1
				Stub Network	10.10.10.4	255.255.255.252	1
				PtP	10.10.10.102	10.10.10.6	1
				PtP	10.10.10.103	10.10.10.10	1
				PtP	10.10.10.104	10.10.10.14	1
				Stub Network	10.10.10.8	255.255.255.252	1
				Stub Network	10.10.10.12	255.255.255.252	1
10.10.10.102	02		3				
				Stub Network	10.10.10.102	255.255.255.255	1
				Stub Network	10.10.10.4	255.255.255.252	1
				PtP	10.10.10.100	10.10.10.5	1
10.10.10.103	02		3				
				Stub Network	10.10.10.103	255.255.255.255	1
				Stub Network	10.10.10.8	255.255.255.252	1
				PtP	10.10.10.100	10.10.10.9	1
10.10.10.104	02		3				
				Stub Network	10.10.10.104	255.255.255.255	1
				Stub Network	10.10.10.12	255.255.255.252	1
				PtP	10.10.10.100	10.10.10.13	1

Once the configuration is performed as shown, enable the OSPF sessions in the core as depicted in the Smartbits OSPF configuration section earlier. Once the neighbor relationship is complete, the DUT will see routes as generated by the core port, as illustrated in Example 15-29.

Example 15-29 *OSPF Verification—Core*

```
DUT#show ip route ospf
     10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
O       10.10.10.8/30 [110/2] via 10.10.10.2, 00:00:11, GigabitEthernet0/2
O       10.10.10.12/30 [110/2] via 10.10.10.2, 00:00:11, GigabitEthernet0/2
O       10.10.10.4/30 [110/2] via 10.10.10.2, 00:00:11, GigabitEthernet0/2
O       10.10.10.104/32 [110/3] via 10.10.10.2, 00:00:11, GigabitEthernet0/2
O       10.10.10.102/32 [110/3] via 10.10.10.2, 00:00:11, GigabitEthernet0/2
O       10.10.10.103/32 [110/3] via 10.10.10.2, 00:00:11, GigabitEthernet0/2
O       10.10.10.100/32 [110/2] via 10.10.10.2, 00:00:11, GigabitEthernet0/2
```

Configuring LDP for L2 VPN

This section provides the procedure for the configuration of LDP with the emulated P router as well as PE routers on the Smartbits 6000 chassis for L2 VPN implementation:

Step 1 To configure LDP, click the **LDP** option in the Navigation pane and expand the same. In the Sessions Grid, configure the following values for the following parameters, as shown in Figure 15-186:

Transport Mode: Router ID

Tester IP Address: 10.10.10.2 (interface IP for tester ingress interface)

Tester Router ID: 10.10.10.100 (loopback interface of P1 router)

SUT IP Address: 10.10.10.1 (interface IP for SUT egress-core interface)

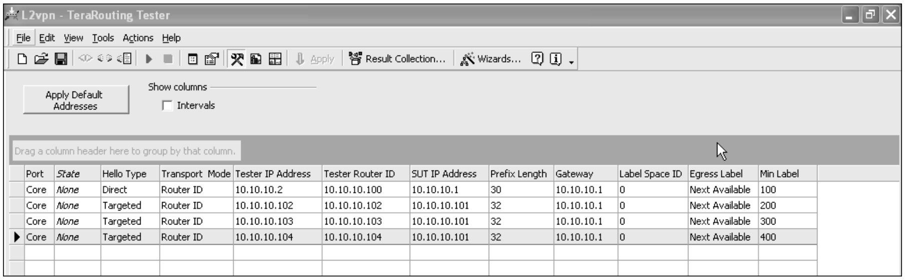
Egress Label: Next Available

Min Label: 100 (configured to avoid overlapping label spaces—default value is 16)

In addition, you must configure targeted LDP sessions between the emulated PE router loopback interfaces and the loopback interface on the PE1 (DUT) router. This is done by the addition of more LDP sessions by right-clicking the grid and selecting the **New Session** option.

For the targeted LDP sessions, the transport mode is configured to be router ID. Tester IP address and tester router ID are configured to be the loopback interface IP of the emulated PE router, and gateway is configured to be 10.10.10.1 (DUT interface IP).

Figure 15-186 *LDP Direct and Targeted Session Configuration*



L2vpn - TeraRouting Tester
File Edit View Tools Actions Help
Apply
Result Collection...
Wizards...
Apply Default Addresses
Show columns
☐ Intervals
Drag a column header here to group by that column.

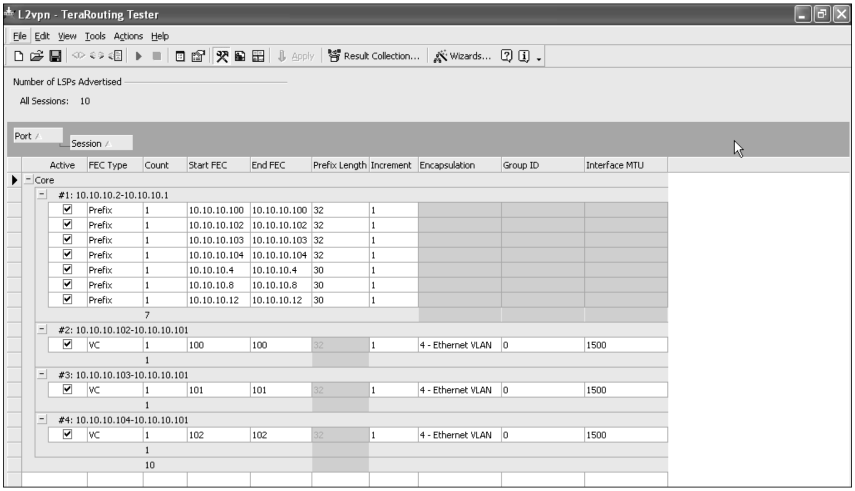
Port	State	Hello Type	Transport Mode	Tester IP Address	Tester Router ID	SUT IP Address	Prefix Length	Gateway	Label Space ID	Egress Label	Min Label
Core	*None*	Direct	Router ID	10.10.10.2	10.10.10.100	10.10.10.1	30	10.10.10.1	0	Next Available	100
Core	*None*	Targeted	Router ID	10.10.10.102	10.10.10.102	10.10.10.101	32	10.10.10.1	0	Next Available	200
Core	*None*	Targeted	Router ID	10.10.10.103	10.10.10.103	10.10.10.101	32	10.10.10.1	0	Next Available	300
Core	*None*	Targeted	Router ID	10.10.10.104	10.10.10.104	10.10.10.101	32	10.10.10.1	0	Next Available	400

Step 2 After the sessions are configured, you must configure the LSPs that need labels assigned to them. For the core, three LSPs are defined to the following three prefixes as advertised by the IGP: 10.10.10.4/30 (link between PE2 and P1),10.10.10.8/30 (link between PE3 and P1), 10.10.10.12/30 (link between PE4 and P1), 10.10.10.100/32 (P1 loopback) and 10.10.10.102/32 (PE2 loopback), 10.10.10.103/32

(PE3 loopback), and 10.10.10.104/32 (PE4 loopback). To configure the LSPs, select the **LSP** tab under LDP in the Navigation pane. Addition of a new LSP is similar to the addition of a new route block advertisement as mentioned earlier in the configuring RIP on Smartbits and configuring BGP on smartbits sections. To add new LSP, right-click the LSP grid and select the **New LSP** option. For the Start FEC and End FEC values, enter the IP addresses that need an LSP assigned, as mentioned earlier, and as shown in Figure 15-187.

To add an LSP for the L2 VPN VC, configure the same under each of the PE targeted sessions as a new LSP. The FEC type is configured to be of type VC. The Start FEC and End FEC values are configured to be the VLAN # associated with the L2 VPN.

Figure 15-187 *LDP LSP Configuration—L2 VPN*



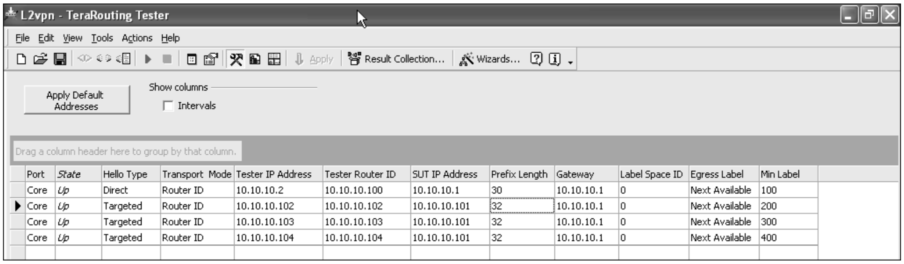
Number of LSPs Advertised

All Sessions: 10

	Active	FEC Type	Count	Start FEC	End FEC	Prefix Length	Increment	Encapsulation	Group ID	Interface MTU
Core										
#1: 10.10.10.2-10.10.10.1										
	☑	Prefix	1	10.10.10.100	10.10.10.100	32	1			
	☑	Prefix	1	10.10.10.102	10.10.10.102	32	1			
	☑	Prefix	1	10.10.10.103	10.10.10.103	32	1			
	☑	Prefix	1	10.10.10.104	10.10.10.104	32	1			
	☑	Prefix	1	10.10.10.4	10.10.10.4	30	1			
	☑	Prefix	1	10.10.10.8	10.10.10.8	30	1			
	☑	Prefix	1	10.10.10.12	10.10.10.12	30	1			
			7							
#2: 10.10.10.102-10.10.10.101										
	☑	VC	1	100	100	32	1	4 - Ethernet VLAN	0	1500
			1							
#3: 10.10.10.103-10.10.10.101										
	☑	VC	1	101	101	32	1	4 - Ethernet VLAN	0	1500
			1							
#4: 10.10.10.104-10.10.10.101										
	☑	VC	1	102	102	32	1	4 - Ethernet VLAN	0	1500
			1							
			10							

Step 3 The final step in the configuration of LDP is to return to the Sessions tab in the Navigation pane and right-click the session in the Sessions grid and select the **Start Router** option. The state of the session will change from Down to Up, as shown in Figure 15-188.

Figure 15-188 *LDP Session States*


L2vpn - TeraRouting Tester
File Edit View Tools Actions Help
Apply
Result Collection...
Wizards...
Apply Default Addresses
Show columns
☐ Intervals
Drag a column header here to group by that column.

Port	State	Hello Type	Transport Mode	Tester IP Address	Tester Router ID	SUT IP Address	Prefix Length	Gateway	Label Space ID	Egress Label	Min Label
Core	Up	Direct	Router ID	10.10.10.2	10.10.10.100	10.10.10.1	30	10.10.10.1	0	Next Available	100
Core	Up	Targeted	Router ID	10.10.10.102	10.10.10.102	10.10.10.101	32	10.10.10.1	0	Next Available	200
Core	Up	Targeted	Router ID	10.10.10.103	10.10.10.103	10.10.10.101	32	10.10.10.1	0	Next Available	300
Core	Up	Targeted	Router ID	10.10.10.104	10.10.10.104	10.10.10.101	32	10.10.10.1	0	Next Available	400

Step 4 Verify the LDP neighbor relationship and label exchange by performing the appropriate commands on the DUT, as shown in Example 15-30.

Example 15-30 *DUT Verification LDP and L2 VPN States*

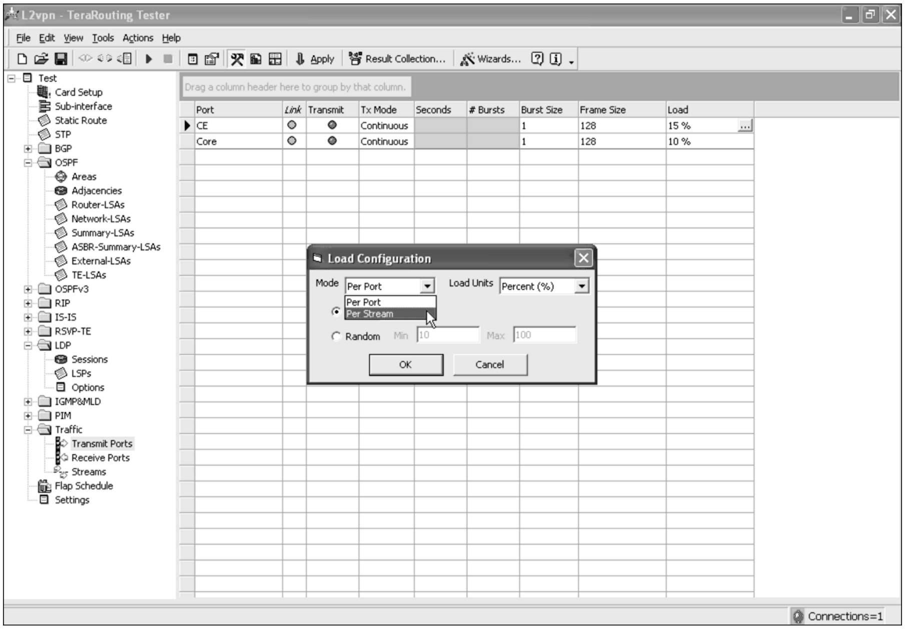
```
DUT#show mpls l2transport vc

Local intf     Local circuit            Dest address    VC ID      Status
------------   ---------------------    --------------  ---------- ----------
Gi0/1.100      Eth VLAN 100             10.10.10.102    100        UP
Gi0/1.101      Eth VLAN 101             10.10.10.103    101        UP
Gi0/1.102      Eth VLAN 102             10.10.10.104    102        UP
DUT#
```

Traffic Generation in L2 VPN

For traffic generation, you are sending three streams originating from the locally connected VLANs on the DUT to the remote PE router loopback interfaces:

Step 1 Select the **Traffic** tab from the Navigation pane and expand the same. Select the **Transmit Ports** tab. In the grid, click the Load column for the core port and set the load to be per stream versus per port in the Load Configuration window on the CE port, as shown in Figure 15-189. Configure the load percentage on the core port to be 10 percent.

Figure 15-189 *Configuring Traffic Load*



Port	Link	Transmit	Tx Mode	Seconds	# Bursts	Burst Size	Frame Size	Load
CE	○	●	Continuous			1	128	15 %
Core	○	●	Continuous			1	128	10 %

Load Configuration

Mode: Per Port (Per Port / Per Stream)

Load Units: Percent (%)

○ Random Min 10 Max 100

Step 2 This step is displayed in Figure 15-190:

2a—Select the **Streams** tab in the Navigation pane.

2b—In the Setup pane, select the **Traffic Wizard** by clicking on the same.

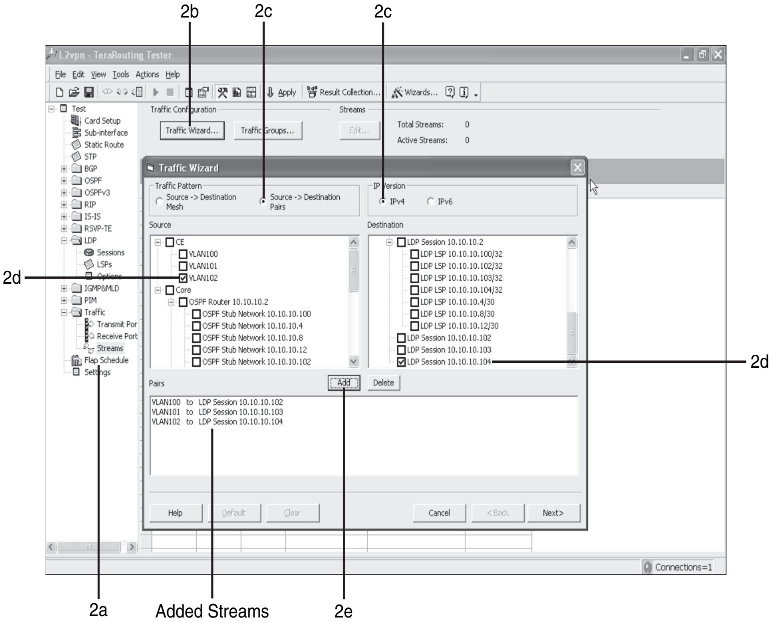
2c—Once the Traffic Wizard window opens, select the traffic pattern to be of type **source > destination pairs** and the IP version to be **IPv4**.

2d—In the Source window, select the **CE VLAN 100** and, in the Destination window, select the core prefix **10.10.10.102/32**.

2e—Finally, click the **Add** button in the Traffic Wizard window to add the new traffic stream.

Repeat this process for each of the streams to be generated from VLAN 101 to prefix 10.10.10.103/32 and VLAN 102 to 10.10.10.104/32.

Figure 15-190 *Adding Streams—CE to Core*



Total Streams: 0
Active Streams: 0

Traffic Pattern: ○ Source -> Destination Mesh ● Source -> Destination Pairs

IP Version: ● IPv4 ○ IPv6

Source
- ☐ CE
  - ☐ VLAN100
  - ☐ VLAN101
  - ☑ VLAN102
- ☐ Core
  - ☐ OSPF Router 10.10.10.2
    - ☐ OSPF Stub Network 10.10.10.100
    - ☐ OSPF Stub Network 10.10.10.4
    - ☐ OSPF Stub Network 10.10.10.8
    - ☐ OSPF Stub Network 10.10.10.12
    - ☐ OSPF Stub Network 10.10.10.102

Destination
- ☐ LDP Session 10.10.10.2
  - ☐ LDP LSP 10.10.10.100/32
  - ☐ LDP LSP 10.10.10.102/32
  - ☐ LDP LSP 10.10.10.103/32
  - ☐ LDP LSP 10.10.10.104/32
  - ☐ LDP LSP 10.10.10.4/30
  - ☐ LDP LSP 10.10.10.8/30
  - ☐ LDP LSP 10.10.10.12/30
- ☐ LDP Session 10.10.10.102
- ☐ LDP Session 10.10.10.103
- ☑ LDP Session 10.10.10.104

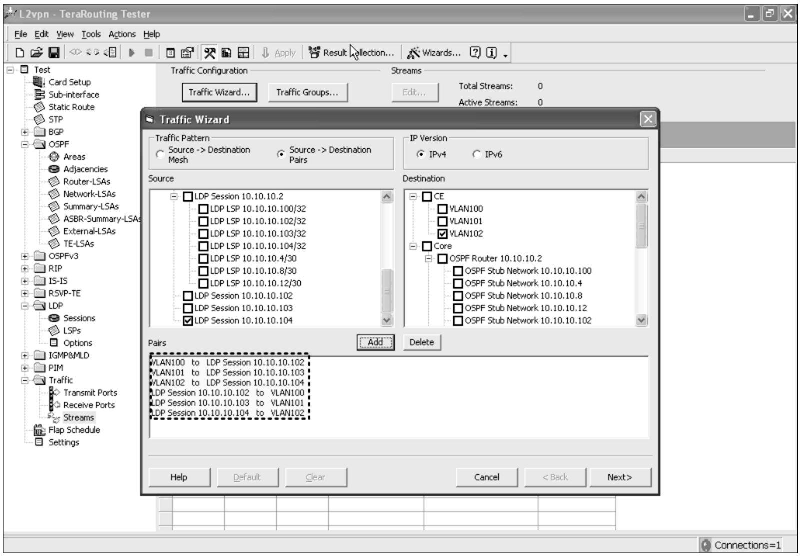
Pairs

```
VLAN100  to  LDP Session 10.10.10.102
VLAN101  to  LDP Session 10.10.10.103
VLAN102  to  LDP Session 10.10.10.104
```

Step 3 Because you want like to create bidirectional streams, configure a second stream by repeating Steps 2c to 2e but with the source as VLAN 100, 101, or 102, respectively, to destinations of LDP sessions 10.10.10.102, 103 or 104, as shown by the highlighted streams in Figure 15-191.

Click **Next** followed by **Finish** in the Traffic Wizard.

Figure 15-191 *Adding Streams—Core to CE*



Traffic Pattern: ○ Source -> Destination Mesh ● Source -> Destination Pairs

IP Version: ● IPv4 ○ IPv6

Source:
☐ LDP Session 10.10.10.2
☐ LDP LSP 10.10.10.100/32
☐ LDP LSP 10.10.10.102/32
☐ LDP LSP 10.10.10.103/32
☐ LDP LSP 10.10.10.104/32
☐ LDP LSP 10.10.10.4/30
☐ LDP LSP 10.10.10.8/30
☐ LDP LSP 10.10.10.12/30
☐ LDP Session 10.10.10.102
☐ LDP Session 10.10.10.103
☑ LDP Session 10.10.10.104

Destination:
☐ CE
☐ VLAN100
☐ VLAN101
☑ VLAN102
☐ Core
☐ OSPF Router 10.10.10.2
☐ OSPF Stub Network 10.10.10.100
☐ OSPF Stub Network 10.10.10.4
☐ OSPF Stub Network 10.10.10.8
☐ OSPF Stub Network 10.10.10.12
☐ OSPF Stub Network 10.10.10.102

Pairs:
VLAN100 to LDP Session 10.10.10.102
VLAN101 to LDP Session 10.10.10.103
VLAN102 to LDP Session 10.10.10.104
LDP Session 10.10.10.102 to VLAN100
LDP Session 10.10.10.103 to VLAN101
LDP Session 10.10.10.104 to VLAN102

Step 4 To correctly configure the traffic for L2 VPN Martini testing, you need to add additional fields into the streams generated from the core port. To do this, click the first stream on the core port in the grid, which opens the Stream Editor window. The first thing to note is that in the Stream Editor, you need to change some parameters under the **Frame Header** tab, as shown in Figure 15-192.

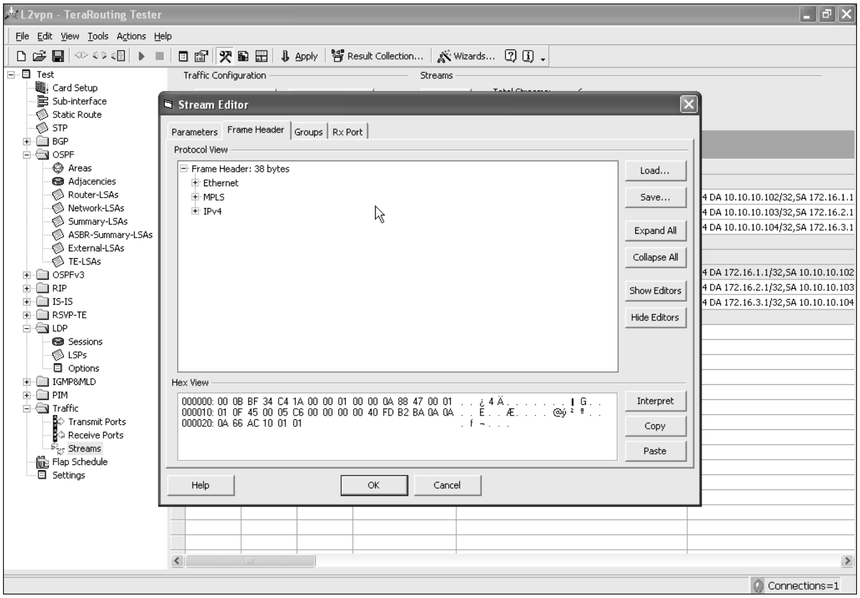
Expand the MPLS drop-down under the frame header and change the IPv4 value (after expanding the same) to the loopback address of the DUT or 10.10.10.101/32, as shown in Figure 15-193.

To configure the streams for L2 VPN testing, you must add an additional MPLS label as well as an Ethernet header and the VLAN field for the Ethernet header, which has not been created. To add a new field, click **Collapse All** in the Stream Editor window and right-click the **MPLS** entry. This gives you an option to insert an MPLS entry, a VLAN entry, an Ethernet entry, and so on. This is shown in Figure 15-194.

Follow the process to insert an MPLS entry that will be denoted by MPLS(2) in the window. Expand the MPLS(2) and the L entry. Change the type to be VC and the FEC to be 100, as shown in Figure 15-195 and Figure 15-196.

Right-click **MPLS (2)** and select the option to **Insert Ethernet**. This creates an entry Ethernet (2). Expand this entry, and, in the destination and source address fields, uncheck the **Use Default** option. Change the address in the destination field to the MAC address of the VLAN 100 interface on the CE port (00-00-01-00-00-09). Insert an arbitrary MAC address in the source MAC address field (00-00-00-12-34-56). This is shown in Figure 15-197.

Figure 15-192 *Changing Parameters in Stream Editor*

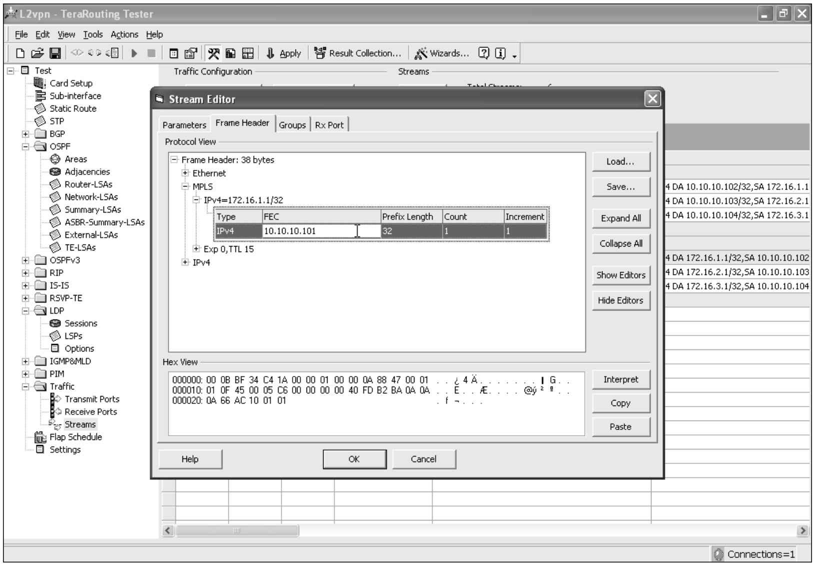


Frame Header: 38 bytes
- Ethernet
- MPLS
- IPv4

```
4 DA 10.10.10.102/32,SA 172.16.1.1
4 DA 10.10.10.103/32,SA 172.16.2.1
4 DA 10.10.10.104/32,SA 172.16.3.1
4 DA 172.16.1.1/32,SA 10.10.10.102
4 DA 172.16.2.1/32,SA 10.10.10.103
4 DA 172.16.3.1/32,SA 10.10.10.104
```

```
000000: 00 0B BF 34 C4 1A 00 00 01 00 00 0A 88 47 00 01   . . ¿ 4 Ä . . . . . . . . ▌ G . .
000010: 01 0F 45 00 05 C6 00 00 00 00 40 FD B2 BA 0A 0A   . . E . . Æ . . . . @ý ² º . .
000020: 0A 66 AC 10 01 01                                 . f ¬ . . .
```

Figure 15-193 *Stream Editor: IPv4 Address Configuration*



Frame Header: 38 bytes
- Ethernet
- MPLS
  - IPv4=172.16.1.1/32

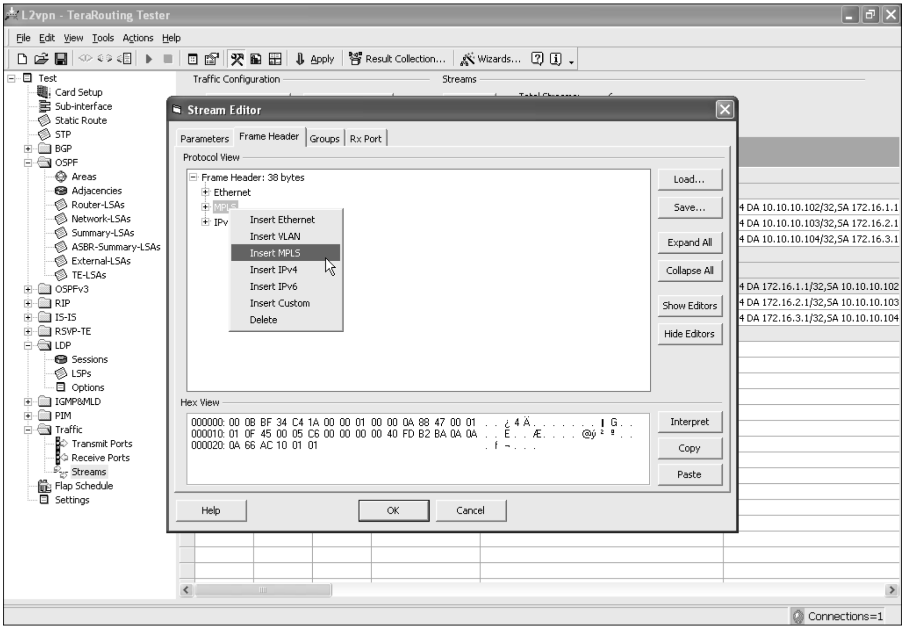
Type	FEC	Prefix Length	Count	Increment
IPv4	10.10.10.101	32	1	1

  - Exp 0,TTL 15
- IPv4

```
4 DA 10.10.10.102/32,SA 172.16.1.1
4 DA 10.10.10.103/32,SA 172.16.2.1
4 DA 10.10.10.104/32,SA 172.16.3.1
4 DA 172.16.1.1/32,SA 10.10.10.102
4 DA 172.16.2.1/32,SA 10.10.10.103
4 DA 172.16.3.1/32,SA 10.10.10.104
```

```
000000: 00 0B BF 34 C4 1A 00 00 01 00 00 0A 88 47 00 01   . . ¿ 4 Ä . . . . . . . . ▌ G . .
000010: 01 0F 45 00 05 C6 00 00 00 00 40 FD B2 BA 0A 0A   . . E . . Æ . . . . @ý ² º . .
000020: 0A 66 AC 10 01 01                                 . f ¬ . . .
```

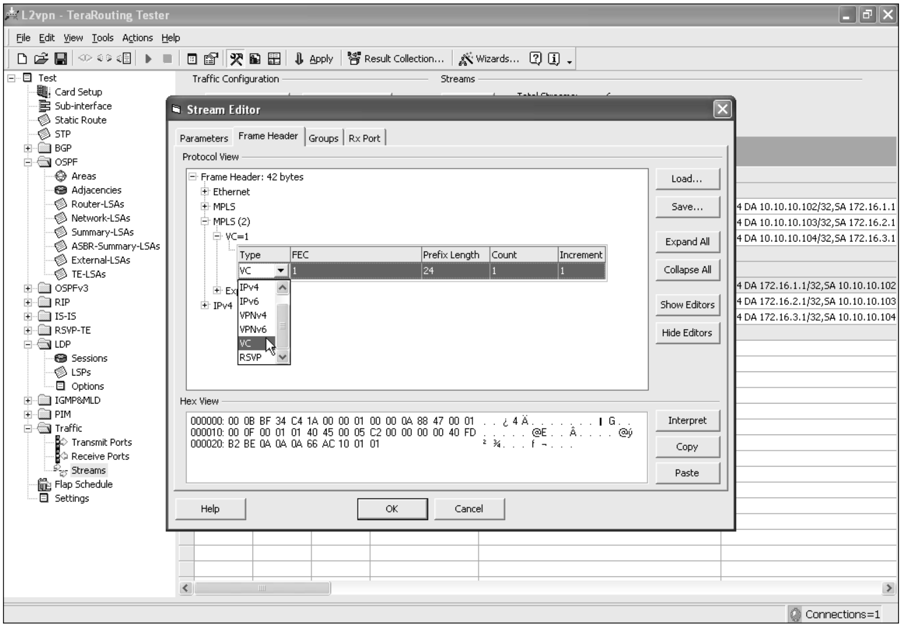
Figure 15-194 *Stream Editor: Adding Additional Fields*



Frame Header: 38 bytes
Ethernet
MPLS
IPv

```
000000: 00 0B BF 34 C4 1A 00 00 01 00 00 0A 88 47 00 01   . . ¿ 4 Ä . . . . . . . ‖ G . .
000010: 01 0F 45 00 05 C6 00 00 00 00 40 FD B2 BA 0A 0A   . . E . . Æ . . . . @ý ² º . .
000020: 0A 66 AC 10 01 01                                 . f ¬ . . .
```

Figure 15-195 *Stream Editor: MPLS VC Label Configuration*

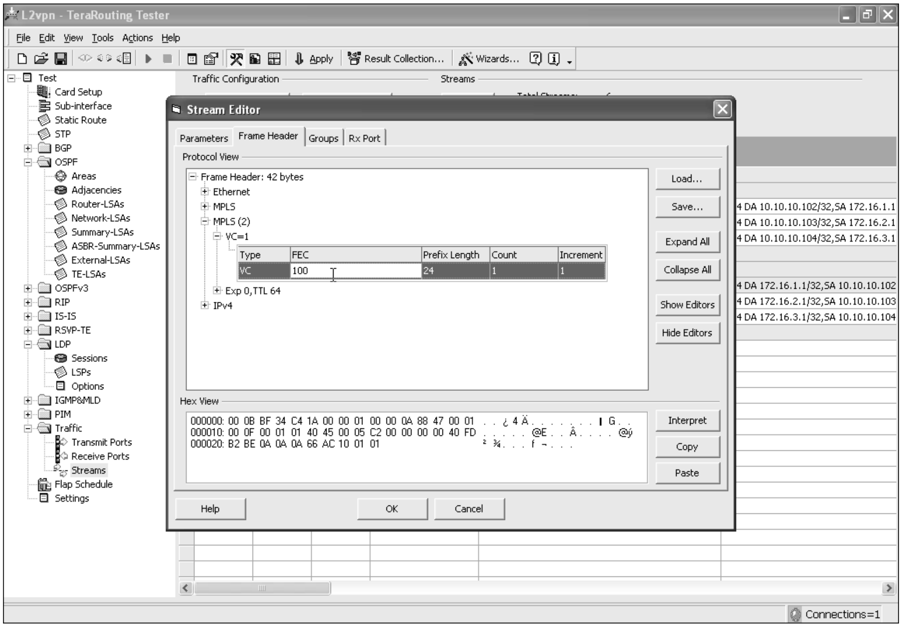


Frame Header: 42 bytes
Ethernet
MPLS
MPLS (2)
VC=1
Ex
IPv4

Type	FEC	Prefix Length	Count	Increment
VC	1	24	1	1

```
000000: 00 0B BF 34 C4 1A 00 00 01 00 00 0A 88 47 00 01   . . ¿ 4 Ä . . . . . . . ‖ G . .
000010: 00 0F 00 01 01 40 45 00 05 C2 00 00 00 00 40 FD   . . . . . . @E . . Â . . . . @ý
000020: B2 BE 0A 0A 0A 66 AC 10 01 01                     ² ¾ . . . f ¬ . . .
```

Figure 15-196 *Stream Editor: VC FEC Configuration*



```
Frame Header: 42 bytes
  Ethernet
  MPLS
  MPLS (2)
    VC=1
```

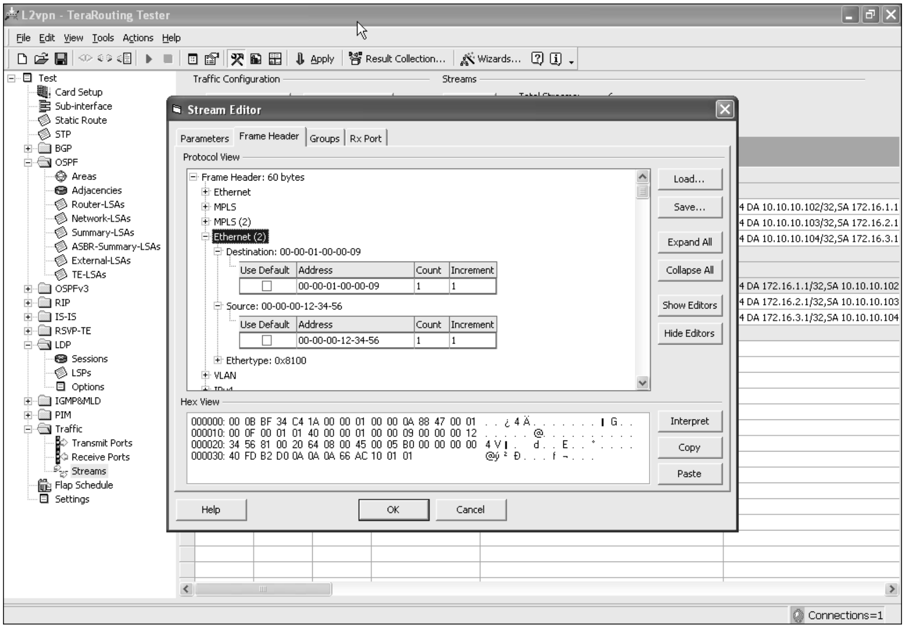
Type	FEC	Prefix Length	Count	Increment
VC	100	24	1	1

```
    Exp 0,TTL 64
  IPv4
```

```
000000: 00 0B BF 34 C4 1A 00 00 01 00 00 0A 88 47 00 01   . . ¿ 4 Ä . . . . . . . . ı G . .
000010: 00 0F 00 01 01 40 45 00 05 C2 00 00 00 00 40 FD   . . . . . . @E . . Â . . . . . @ý
000020: B2 BE 0A 0A 0A 66 AC 10 01 01                     ² ¾ . . . f ¬ . . . .
```

```
4 DA 10.10.10.102/32,SA 172.16.1.1
4 DA 10.10.10.103/32,SA 172.16.2.1
4 DA 10.10.10.104/32,SA 172.16.3.1
4 DA 172.16.1.1/32,SA 10.10.10.102
4 DA 172.16.2.1/32,SA 10.10.10.103
4 DA 172.16.3.1/32,SA 10.10.10.104
```

Figure 15-197 *Stream Editor: Ethernet (2) Configuration*



```
Frame Header: 60 bytes
  Ethernet
  MPLS
  MPLS (2)
  Ethernet (2)
    Destination: 00-00-01-00-00-09
```

Use Default	Address	Count	Increment
☐	00-00-01-00-00-09	1	1

```
    Source: 00-00-00-12-34-56
```

Use Default	Address	Count	Increment
☐	00-00-00-12-34-56	1	1

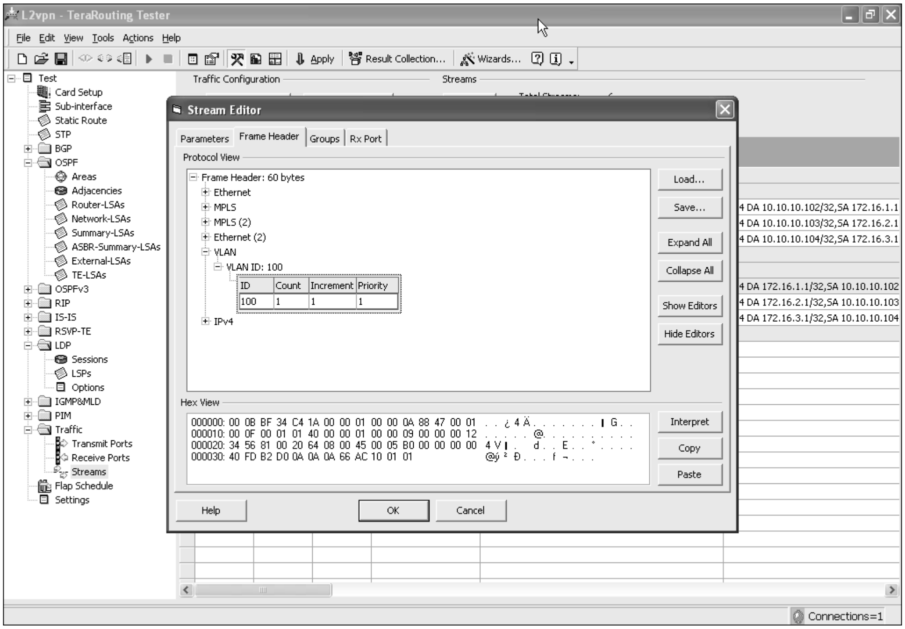
```
    Ethertype: 0x8100
  VLAN
```

```
000000: 00 0B BF 34 C4 1A 00 00 01 00 00 0A 88 47 00 01   . . ¿ 4 Ä . . . . . . . . ı G . .
000010: 00 0F 00 01 01 40 00 00 01 00 00 09 00 00 00 12   . . . . . . @ . . . . . . . . . .
000020: 34 56 81 00 20 64 08 00 45 00 05 B0 00 00 00 00   4 V ı . . d . . E . . ° . . . . .
000030: 40 FD B2 D0 0A 0A 0A 66 AC 10 01 01               @ý ² Ð . . . f ¬ . . . .
```

```
4 DA 10.10.10.102/32,SA 172.16.1.1
4 DA 10.10.10.103/32,SA 172.16.2.1
4 DA 10.10.10.104/32,SA 172.16.3.1
4 DA 172.16.1.1/32,SA 10.10.10.102
4 DA 172.16.2.1/32,SA 10.10.10.103
4 DA 172.16.3.1/32,SA 10.10.10.104
```

Right-click **Ethernet (2)** and select the option to **Insert VLAN**. Expand the VLAN and check to see if the VLAN number is configured to be 100, as displayed in Figure 15-198.

Figure 15-198 *Stream Editor: VLAN (2) Configuration*



Frame Header: 60 bytes
- Ethernet
- MPLS
- MPLS (2)
- Ethernet (2)
- VLAN
  - VLAN ID: 100
- IPv4

ID	Count	Increment	Priority
100	1	1	1

```
000000: 00 0B BF 34 C4 1A 00 00 01 00 00 0A 88 47 00 01  . . ¿ 4 Ä . . . . . . . ▌ G . .
000010: 00 0F 00 01 01 40 00 00 01 00 00 09 00 00 00 12  . . . . . @. . . . . . . . . .
000020: 34 56 81 00 20 64 08 00 45 00 05 B0 00 00 00 00  4 V ▌ .   d . . E . . ° . . . .
000030: 40 FD B2 D0 0A 0A 0A 66 AC 10 01 01              @ý ² Ð . . . f ¬ . . .
```

```
4 DA 10.10.10.102/32,SA 172.16.1.1
4 DA 10.10.10.103/32,SA 172.16.2.1
4 DA 10.10.10.104/32,SA 172.16.3.1
4 DA 172.16.1.1/32,SA 10.10.10.102
4 DA 172.16.2.1/32,SA 10.10.10.103
4 DA 172.16.3.1/32,SA 10.10.10.104
```

Click **OK** in the Stream Editor to complete the configuration.

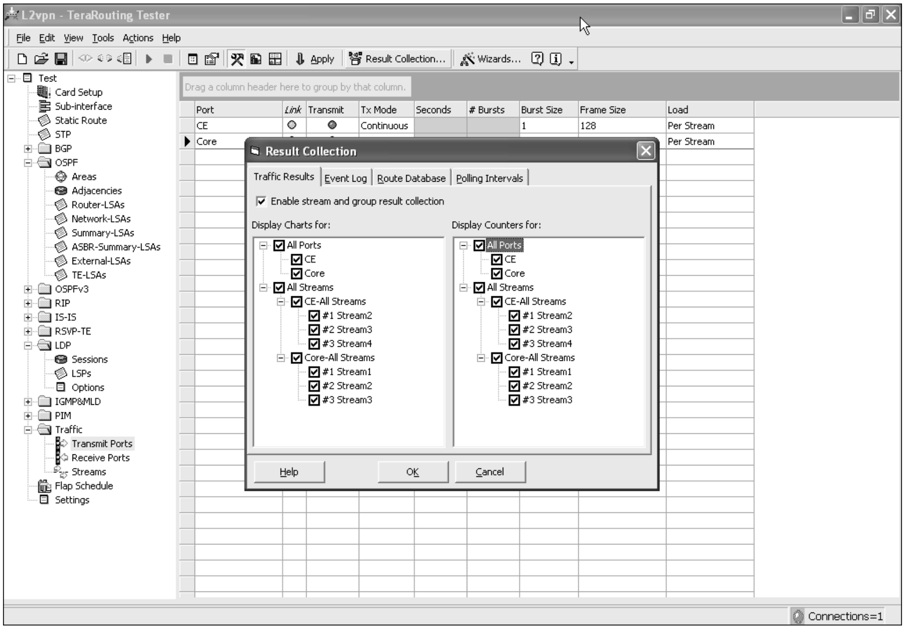
Step 5 Repeat the previous corrective steps for all three streams to be generated by the core port. Signatures can be configured for each of the streams by double-clicking the streams in the grid to open the Stream Editor window. Select the **Parameters** tab and select the **Include Signature Field** option, as shown earlier in Figure 15-180, and click **OK**.

Step 6 Go back to the Transmit tab in the Navigation pane. Prior to traffic generation, click the **Result Collection** button in the Setup pane and select all ports and all streams to be enabled for displaying charts as well as counters in the Result Collection window, as shown in Figure 15-199. Click **OK** to close the Result Collection window. Highlight both ports in the grid and right-click and select the **Start Traffic** option.

Step 7 Once the streams have started, verify operation by checking the stream counters in the Result window after stopping the streams, as shown in Figure 15-200.

The main reason for addition of signatures is to avoid the addition of control plane traffic not pertaining to the stream to be added into the Rx.

Figure 15-199 *Configuring Result Collection per Stream*



Port	Link	Transmit	Tx Mode	Seconds	# Bursts	Burst Size	Frame Size	Load
CE	○	●	Continuous			1	128	Per Stream
Core								Per Stream

Result Collection

Traffic Results | Event Log | Route Database | Polling Intervals

☑ Enable stream and group result collection

Display Charts for:

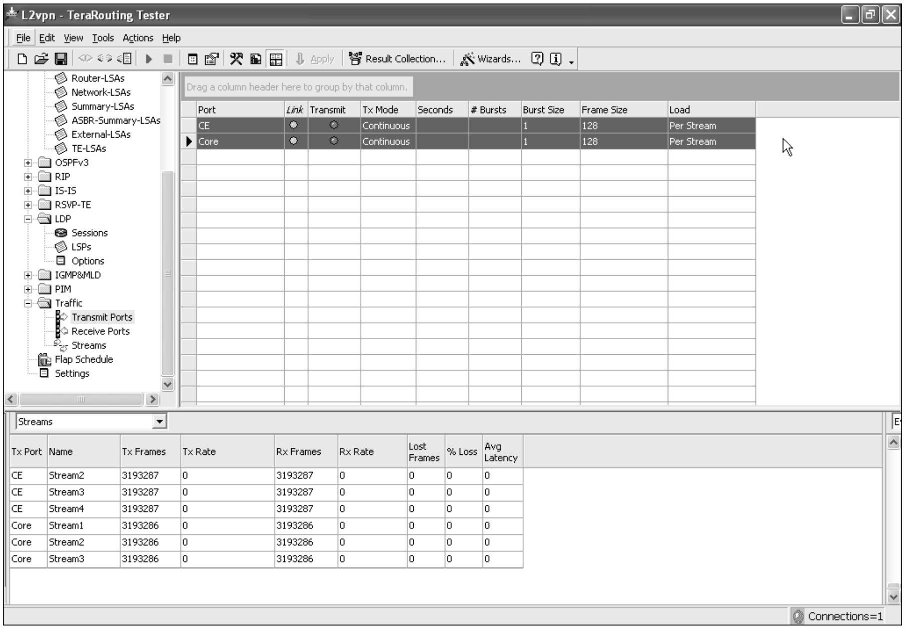
- ☑ All Ports
  - ☑ CE
  - ☑ Core
- ☑ All Streams
  - ☑ CE-All Streams
    - ☑ #1 Stream2
    - ☑ #2 Stream3
    - ☑ #3 Stream4
  - ☑ Core-All Streams
    - ☑ #1 Stream1
    - ☑ #2 Stream2
    - ☑ #3 Stream3

Display Counters for:

- ☑ All Ports
  - ☑ CE
  - ☑ Core
- ☑ All Streams
  - ☑ CE-All Streams
    - ☑ #1 Stream2
    - ☑ #2 Stream3
    - ☑ #3 Stream4
  - ☑ Core-All Streams
    - ☑ #1 Stream1
    - ☑ #2 Stream2
    - ☑ #3 Stream3

Help | OK | Cancel

Figure 15-200 *Verification of Traffic Generation*



Port	Link	Transmit	Tx Mode	Seconds	# Bursts	Burst Size	Frame Size	Load
CE	○	○	Continuous			1	128	Per Stream
Core	○	○	Continuous			1	128	Per Stream

Tx Port	Name	Tx Frames	Tx Rate	Rx Frames	Rx Rate	Lost Frames	% Loss	Avg Latency
CE	Stream2	3193287	0	3193287	0	0	0	0
CE	Stream3	3193287	0	3193287	0	0	0	0
CE	Stream4	3193287	0	3193287	0	0	0	0
Core	Stream1	3193286	0	3193286	0	0	0	0
Core	Stream2	3193286	0	3193286	0	0	0	0
Core	Stream3	3193286	0	3193286	0	0	0	0