BGP-MPLS VPN (RFC-2547bis) Functional Testing

Application Note

MPLS Virtual Private Networks (VPNs) in RFC-2547bis defines a mechanism by which service providers can use their IP backbones to provide VPN services to customers. A VPN is a set of sites which share common routing information and whose connectivity is controlled by a collection of policies. RFC-2547bis VPNs are also known as BGP-MPLS VPNs because the Border Gateway Protocol (BGP) is used to distribute VPN routing information across the provider's backbone, and MPLS is used to establish virtual circuits and to forward VPN traffic across the backbone to remote VPN sites.

Agilent Technologies

The Basics of BGP-MPLS VPNs

A VPN consists of two topological areas: the provider's network and the customer's network. The provider's network consists of edge routers that provide VPN services and connect to the customer's network (i.e. Provider Edge (PE) routers) as well as routers that provide other services (i.e. provider core (P) routers). The customer's network is commonly distributed across multiple physical sites. Customer routers that connect to the provider network are called Customer Edge (CE) routers as shown in figure 1.

A provider can manage multiple VPNs as long as the policies are able to keep routes separate from different VPNs. Similarly, a site can belong to multiple VPNs as long as it keeps routes from the different VPNs separate.

The connection between the CE and PE routers can be a remote (WAN) or a direct connection such as a Frame Relay, ATM PVC, or Ethernet (VLAN) connection. Customer networks exchange routes with provider networks (CE to PE connections) using static routes or via routing peering sessions (e.g. E-BGP, RIP, or OSPF).

CE routers establish routing peering sessions with PE routers using routing protocols (RIP or OSPF). Static routes could also be used. Routing peering sessions exchange routes between CE and PE routers. Once the PE router receives CE route updates, it has to create a VPN routing and forwarding table (VRF table) for each VPN site connected to that router.

PE routers establish MP-iBGP sessions to exchange the customer routes reachability information. Traffic traverses the provider's network over pre-established label switched paths (LSPs) which are set up using LDP or RSVP-TE signaling protocols. The PE router adds a two-label prefix to each packet of the customer's IP data traffic. The outer label identifies the next-hop router along the LSP in the provider's network, while the inner label identifies the particular VPN customer connected at the destination router. Label information is exchanged during the MP-iBGP session setup.

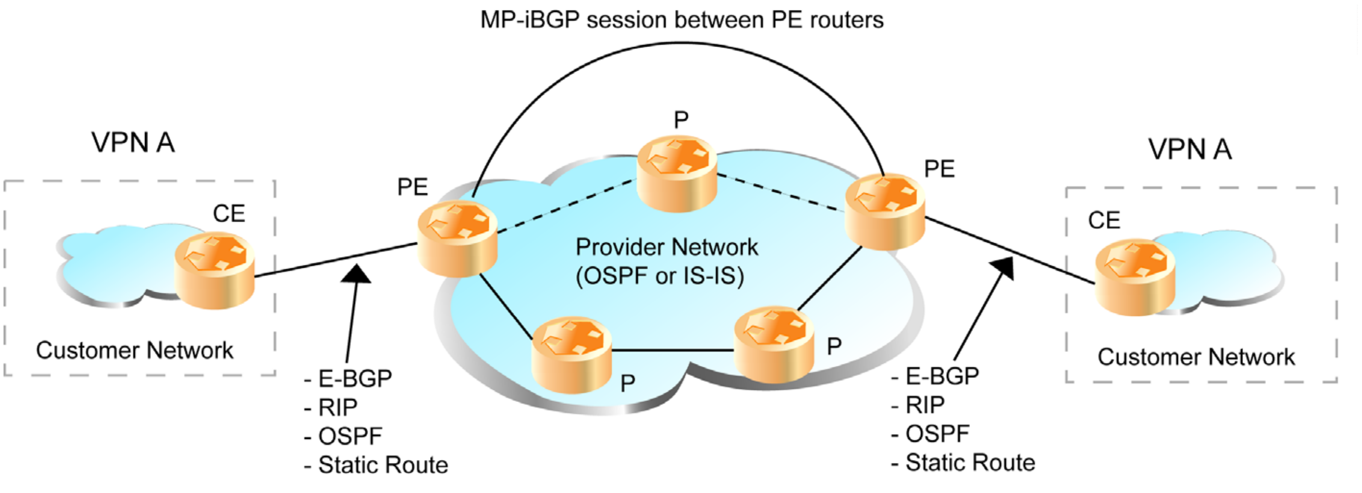


Figure 1: BGP-MPLS VPNs layout

PE	Provider Edge router
CE	Customer Edge router
P	Provider Core router
- - -	Label Switched Path (LSP)
——	Physical Link

Test Challenges

BGP-MPLS VPNs are complex technology incorporating several interacting protocols, including internal gateway protocols (IGP) with traffic engineering extensions (i.e. OSPF-TE and ISIS-TE), multi-protocol iBGP (MP-iBGP), and MPLS signaling protocols (i.e. LDP/CR-LDP, RSVP-TE). The complexity of BGP-MPLS VPN along with the immaturity of the protocols driving this new service makes testing the devices and networks a challenging and essential task.

Testing BGP-MPLS VPNs requires a test solution with a wide breadth of protocol emulations including RIP, OSPF-TE, ISIS-TE, BGP-4, MP-iBGP, LDP/CR-LDP, and RSVP-TE. To evaluate the scalability and performance of BGP-MPLS VPNs, the test solution must also feature multi-port, wire-speed MPLS traffic generation and analysis.

BGP-MPLS VPN Setup and Functional Test

As described in RFC-2547bis, the PE router is a key element as it features the intelligence and the configuration complexity (i.e. policies) that enable connectivity between various VPN sites.

To effectively verify the functionality of PE routers, it is necessary to examine how reliably the router can establish LSPs between different PE routers, and whether the router can employ MP-iBGP sessions to exchange VPN route and reachability information of the different VPN sites, and build VPN routing and forwarding tables (VRFs).

The Agilent RouterTester simulates an IGP (RIP, OSPF, or IS-IS) network topology behind the system under test and generates LDP and RSVP-TE signaling messages to the SUT to test the ability to establish LSPs. RouterTester opens and maintains MP-iBGP sessions with the SUT.

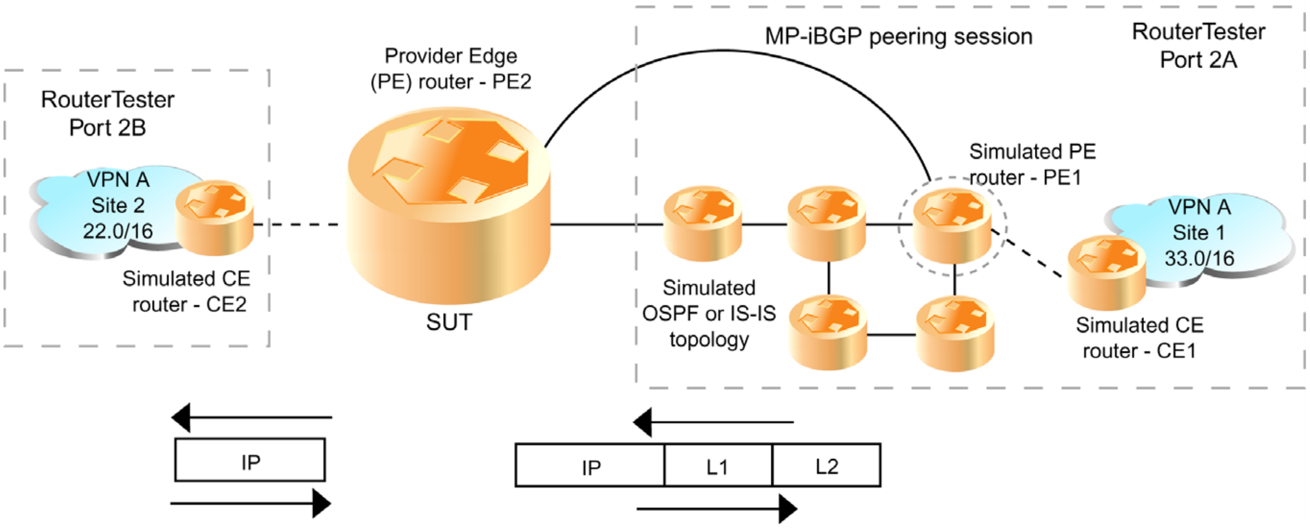
The following section examines how effectively RouterTester verifies the setup and functionality of BGP-MPLS VPN networks.

Procedure: The router under test is configured as a provider edge (PE) router in a BGP-MPLS virtual private network.

Two RouterTester ports are needed to execute this test. One test port generates OSPF or IS-IS routing protocol updates to the SUT to simulate a provider network topology. The simulated provider network is comprised of a mesh of provider core (P) routers and provider edge (PE) routers. On the same test port, CE router is also configured to simulate a customer site in the VPN.

The second test port simulates a second CE router and generates OSPF routes, effectively simulating another customer site in the VPN (refer to figure 2).

Figure 2: BGP-MPLS VPNs setup test


RouterTester Port 2B
VPN A Site 2 22.0/16
Simulated CE router - CE2
Provider Edge (PE) router - PE2
SUT
MP-iBGP peering session
RouterTester Port 2A
Simulated PE router - PE1
VPN A Site 1 33.0/16
Simulated CE router - CE1
Simulated OSPF or IS-IS topology
IP
IP
L1
L2

As per the configuration, the SUT and the simulated PE router establish an MP-iBGP session. RouterTester generates LDP or RSVP-TE signaling protocol messages to the SUT to establish LSPs which carry data traffic between customer sites in the VPN. Once the MP-iBGP session and LSPs are up, the first test port sends a stream of two-deep labeled packets from the simulated PE router, through the SUT, to addresses simulated behind the second RouterTester port (acting as the CE router). This represents traffic going from end to end in the VPN. The SUT pops the two-level labels from the packets and forwards them to the CE router. The SUT's ability to push two-deep label stacks is then tested by sending unlabeled traffic from the second test port (simulated CE router) to the SUT. The SUT pushes two labels onto each packet and forwards the traffic to the adjacent PE router over the pre-established LSP.

Steps to Perform BGP-MPLS VPN Functionality Test

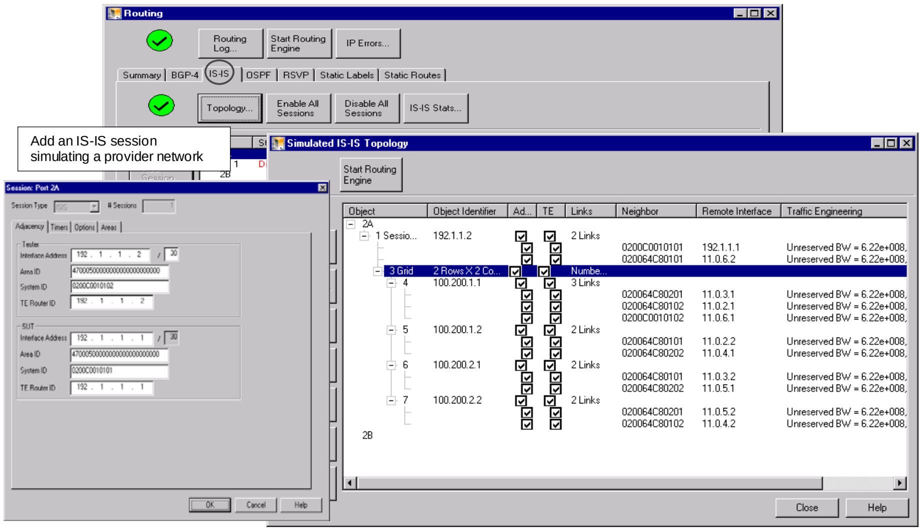
In this test, we use one VPN (VPN A) that has two sites (site 1 and 2).

Control Plane Configuration Setup

1. An OSPF (or IS-IS) network topology is simulated behind RouterTester ports 2A emulating the provider's network (as shown in figure 2 and 3).

2. An MP-iBGP session is set up between the SUT (PE2) and a selected simulated PE router (PE1) as shown in figure 4.

3. The SUT is configured with the appropriate settings to create the virtual private network. Figure 5 shows how to create the provider's VPN on RouterTester. The import route target, which defines the import behavior of the simulated PE router, is configured. Figure 5 also shows how to create the simulated customer site (CE1) with the appropriate route distinguisher (RD). This RD is used to create the VPN-IPv4 addresses that are advertised to the SUT (through the MP-iBGP session).



Add an IS-IS session simulating a provider network

Session: Port 2A

Session Type: ISIS # Sessions: 1

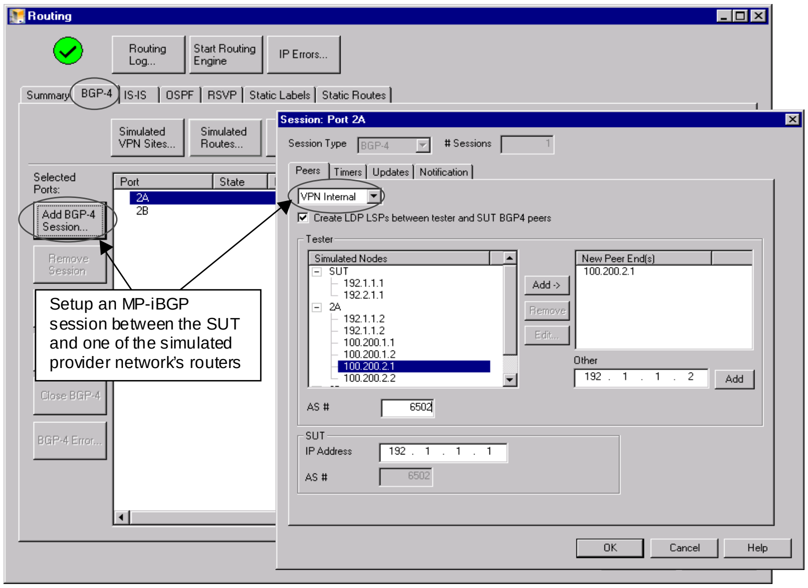
Adjacency | Timers | Options | Areas

Tester
Interface Address: 192 . 1 . 1 . 2 / 30
Area ID: 4700050000000000000000000
System ID: 0200C0010102
TE Router ID: 192 . 1 . 1 . 2

SUT
Interface Address: 192 . 1 . 1 . 1 / 30
Area ID: 4700050000000000000000000
System ID: 0200C0010101
TE Router ID: 192 . 1 . 1 . 1

Object	Object Identifier	Ad...	TE	Links	Neighbor	Remote Interface	Traffic Engineering
2A							
1 Sessio...	192.1.1.2	☑	☑	2 Links			
		☑	☑		0200C0010101	192.1.1.1	Unreserved BW = 6.22e+008,
		☑	☑		020064C80101	11.0.6.2	Unreserved BW = 6.22e+008,
3 Grid	2 Rows X 2 Co...	☑	☑	Numbe...			
4	100.200.1.1	☑	☑	3 Links			
		☑	☑		020064C80201	11.0.3.1	Unreserved BW = 6.22e+008,
		☑	☑		020064C80102	11.0.2.1	Unreserved BW = 6.22e+008,
		☑	☑		0200C0010102	11.0.6.1	Unreserved BW = 6.22e+008,
5	100.200.1.2	☑	☑	2 Links			
		☑	☑		020064C80101	11.0.2.2	Unreserved BW = 6.22e+008,
		☑	☑		020064C80202	11.0.4.1	Unreserved BW = 6.22e+008,
6	100.200.2.1	☑	☑	2 Links			
		☑	☑		020064C80101	11.0.3.2	Unreserved BW = 6.22e+008,
		☑	☑		020064C80202	11.0.5.1	Unreserved BW = 6.22e+008,
7	100.200.2.2	☑	☑	2 Links			
		☑	☑		020064C80201	11.0.5.2	Unreserved BW = 6.22e+008,
		☑	☑		020064C80102	11.0.4.2	Unreserved BW = 6.22e+008,
2B							

Figure 3: Add an IS-IS network topology behind port 2A



Setup an MP-iBGP session between the SUT and one of the simulated provider network's routers

Session: Port 2A

Session Type: BGP-4 # Sessions: 1

Peers | Timers | Updates | Notification

VPN Internal

☑ Create LDP LSPs between tester and SUT BGP4 peers

Tester

Simulated Nodes:
- SUT
  - 192.1.1.1
  - 192.2.1.1
- 2A
  - 192.1.1.2
  - 192.1.1.2
  - 100.200.1.1
  - 100.200.1.2
  - 100.200.2.1
  - 100.200.2.2

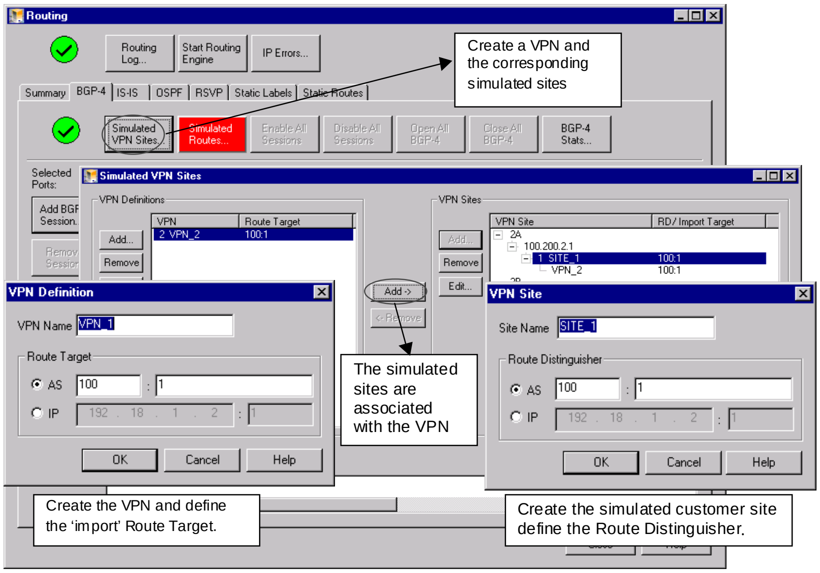
New Peer End(s): 100.200.2.1

Other: 192 . 1 . 1 . 2

AS #: 6502

SUT
IP Address: 192 . 1 . 1 . 1
AS #: 6502

Figure 4: Add an MP-iBGP session between the SUT (PE2) and a simulated PE (PE1)



Create a VPN and the corresponding simulated sites

VPN Definitions:

VPN	Route Target
2 VPN_2	100:1

VPN Sites:

VPN Site	RD / Import Target
2A	
100.200.2.1	
1 SITE_1	100:1
VPN_2	100:1

VPN Definition
VPN Name: VPN_1
Route Target
● AS 100 : 1
○ IP 192 . 18 . 1 . 2 : 1

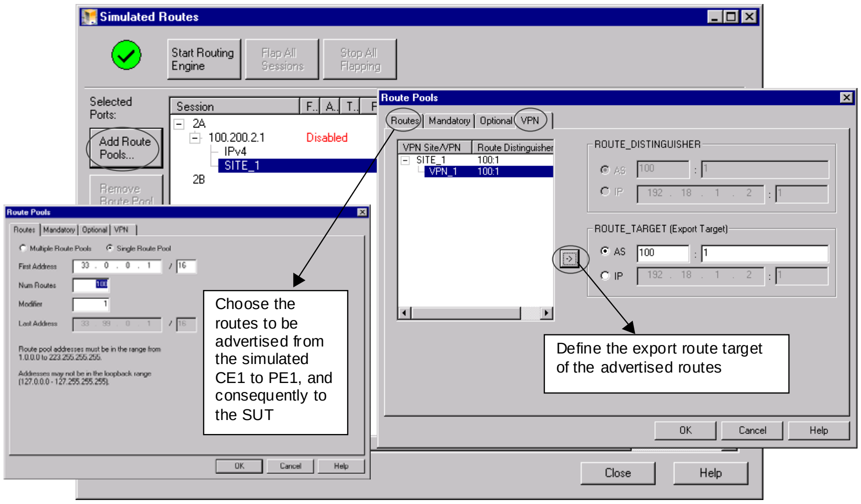
The simulated sites are associated with the VPN

VPN Site
Site Name: SITE_1
Route Distinguisher
● AS 100 : 1
○ IP 192 . 18 . 1 . 2 : 1

Create the VPN and define the 'import' Route Target.

Create the simulated customer site define the Route Distinguisher.

Figure 5: Create a VPN and a simulated customer site



Route Pools: ○ Multiple Route Pools ● Single Route Pool

First Address: 33 . 0 . 0 . 1 / 16

Num Routes: 100

Modifier: 1

Last Address: 33 . 99 . 0 . 1 / 16

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).

VPN Site/VPN	Route Distinguisher
SITE_1	100:1
VPN_1	100:1

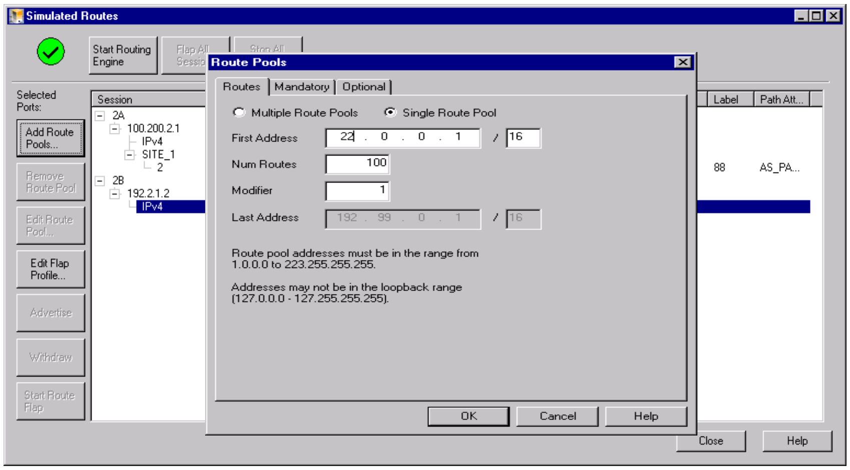
ROUTE_DISTINGUISHER: ● AS 100 : 1 ○ IP 192 . 18 . 1 . 2 : 1

ROUTE_TARGET (Export Target): ● AS 100 : 1 ○ IP 192 . 18 . 1 . 2 : 1

Choose the routes to be advertised from the simulated CE1 to PE1, and consequently to the SUT

Define the export route target of the advertised routes

Figure 6: Advertise routes to the SUT using the simulated PE1 and CE1 routers



○ Multiple Route Pools ● Single Route Pool

First Address: 22 . 0 . 0 . 1 / 16

Num Routes: 100

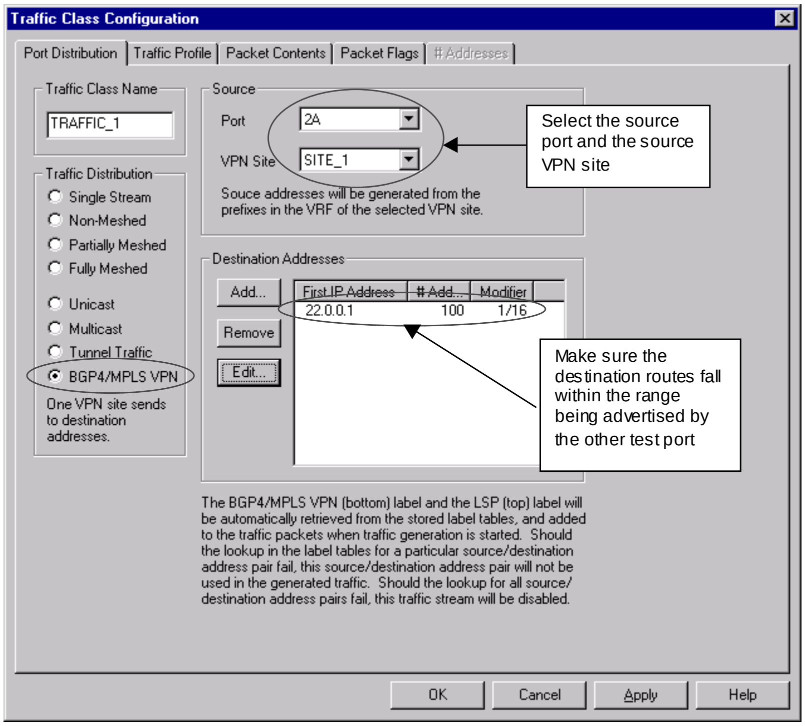
Modifier: 1

Last Address: 192 . 99 . 0 . 1 / 16

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 7: Advertise routes behind port 2B (E-BGP protocol is used in this case)



Traffic Class Name: TRAFFIC_1

Source: Port 2A; VPN Site SITE_1

Souce addresses will be generated from the prefixes in the VRF of the selected VPN site.

Traffic Distribution:
○ Single Stream
○ Non-Meshed
○ Partially Meshed
○ Fully Meshed

○ Unicast
○ Multicast
○ Tunnel Traffic
● BGP4/MPLS VPN

One VPN site sends to destination addresses.

Destination Addresses:

First IP Address	# Add...	Modifier
22.0.0.1	100	1/16

The BGP4/MPLS VPN (bottom) label and the LSP (top) label will be automatically retrieved from the stored label tables, and added to the traffic packets when traffic generation is started. Should the lookup in the label tables for a particular source/destination address pair fail, this source/destination address pair will not be used in the generated traffic. Should the lookup for all source/destination address pairs fail, this traffic stream will be disabled.

Select the source port and the source VPN site

Make sure the destination routes fall within the range being advertised by the other test port

Figure 8: Configure the traffic stream to be sent from one customer (CE1) site to the other (CE2)

4. Route pools (e.g. 33.0/16) are configured along with the Route Distinguisher (RD). The route pools are advertised to the SUT (PE2) representing routes behind the simulated VPN customer edge router on site 1 (CE1), as shown in figure 6.

5. RouterTester port (2B) simulates the second customer site (CE2) in the VPN. Port 2B injects routes (e.g. 22.0/16) into the SUT using either static routes or any IP routing protocols (e.g. OSPF, RIP, E-BGP), as shown in figure 7.

6. After starting the routing engine, the SUT and the simulated PE routers exchange routes (via the MP-iBGP session). This process ensures that the bottom label value (i.e. VPN label) for the session and the corresponding VRFs are populated. The SUT is also prompted to open an LDP (or RSVP-TE) LSP to RouterTester port 2A. Label values (i.e. the top label value) are exchanged during the LDP session.

7. Using the SUT's commands, populated VRFs can be examined on the SUT to verify the router's ability to correctly populate its VRFs.

Data plane (traffic) configuration

1. Data traffic is sent from Port 2A destined to the simulated routes behind port 2B. This data traffic simulates traffic going from customer site 1 (CE1) to customer site 2 (CE2). The transmitted data traffic has two-deep label. The bottom label is the VPN label and the top label is the LSP label. Note: The destination address of the stream should fall within the range of the simulated route pool on port 2B (e.g. 22.0/16) as shown in figure 8.

2. Port 2B monitors the received traffic to verify that the labels have been popped by the SUT.

3. Plain IP data traffic is sent from Port 2B destined to routes simulated behind port 2A (e.g. 33.0/16). This unicast traffic is plain IP packets with no labels; and represents traffic going from customer site 2 (CE2) to customer site 1 (CE1) through the provider's VPN.

4. Port 2A monitors the received traffic to verify that the SUT is pushing the correct two-deep labels onto packets.

References

BGP-MPLS VPNs (draft-ietf-ppvpn-rfc2547bis-xx.txt, July, 2001)

Multi-protocol Label Switching Architecture (RFC 3031, January, 2001)

Carrying Label Information in BGP-4 (RFC 3107, May, 2001)

LDP Specification (RFC 3036, January, 2001)

MPLS and VPN Architectures (Jim Guichard and Ivan Pepelnjak, Cisco Press, December, 2000)

MPLS: Technology and Applications (Bruce Davie, Yakov Rekhter, September, 2000)

Service requirements for Provider Provisioned Virtual Private Networks
(draft-ietf-ppvpn-requirements-xx, August, 2001)

This page intentionally left blank.

Agilent IP Routing Test Solution

Agilent's IP Routing Test Solution product family includes Agilent QA Robot and Agilent RouterTester and the test software that runs on these platforms. The QA Robot provides all basic IP routing test capabilities, plus conformance, stress and functional testing. The RouterTester is enhanced with wire-speed traffic generation that enables comprehensive performance metrics and integrated routing protocol support.

www.agilent.com/comms/RouterTester

United States:

Agilent Technologies
Test and Measurement Call Center
P.O. Box 4026
Englewood, CO 80155-4026
1-800-452-4844

Canada:

Agilent Technologies Canada Inc.
5150 Spectrum Way
Mississauga, Ontario
L4W 5G1
1-877-894-4414

Europe:

Agilent Technologies
European Marketing Organisation
P.O. Box 999
1180 AZ Amstelveen
The Netherlands
(31 20) 547-9999

Japan:

Agilent Technologies Japan Ltd.
Measurement Assistance Center
9-1, Takakura-Cho, Hachioji-Shi,
Tokyo 192-8510, Japan
Tel: (81) 426-56-7832
Fax: (81) 426-56-7840

Latin America:

Agilent Technologies
Latin American Region Headquarters
5200 Blue Lagoon Drive, Suite #950
Miami, Florida 33126
U.S.A.
Tel: (305) 267-4245
Fax: (305) 267-4286

Asia Pacific:

Agilent Technologies
19/F, Cityplaza One, 1111 King's Road,
Taikoo Shing, Hong Kong, SAR
Tel: (852) 2599-7889
Fax: (852) 2506-9233

Australia/New Zealand:

Agilent Technologies Australia Pty Ltd
347 Burwood Highway
Forest Hill, Victoria 3131
Tel: 1-800-629-485 (Australia)
Fax: (61-3) 9272-0749
Tel: 0-800-738-378 (New Zealand)
Fax: (64-4) 802-6881

Specifications subject to change
October 18, 2001
5988-4561EN

Agilent Technologies