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

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.
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
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](image-url)
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).
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.
BGP-MPLS VPN Protocol Software

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)
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