About the Multiprotocol Label Switching/Virtual Private Network Border Gateway Protocol Login Event Generator

Published: May 27, 2013

Introduction

The Service Control Management Suite (SCMS) Subscriber Manager (SM) Multiprotocol Label Switching (MPLS)/Virtual Private Network (VPN) Border Gateway Protocol (BGP) Login Event Generator (LEG) is a software module that dynamically provides the MPLS label for each VPN using the BGP. It listens to the BGP traffic to determine the correct MPLS label.

- MPLS/VPN Overview, page 27-1
- MPLS/VPN BGP LEG Overview, page 27-2

MPLS/VPN Overview

Internet service providers that have a common network of multiple server sites with IP interconnectivity deployed on a shared infrastructure can be securely connected using a Virtual Private Network (VPN). A VPN can secure a shared network connection by employing technologies such as authentication, encryption, and tunneling. The VPN traffic is encapsulated and transparently sent from one site to another enabling the traffic to be secured by encryption.

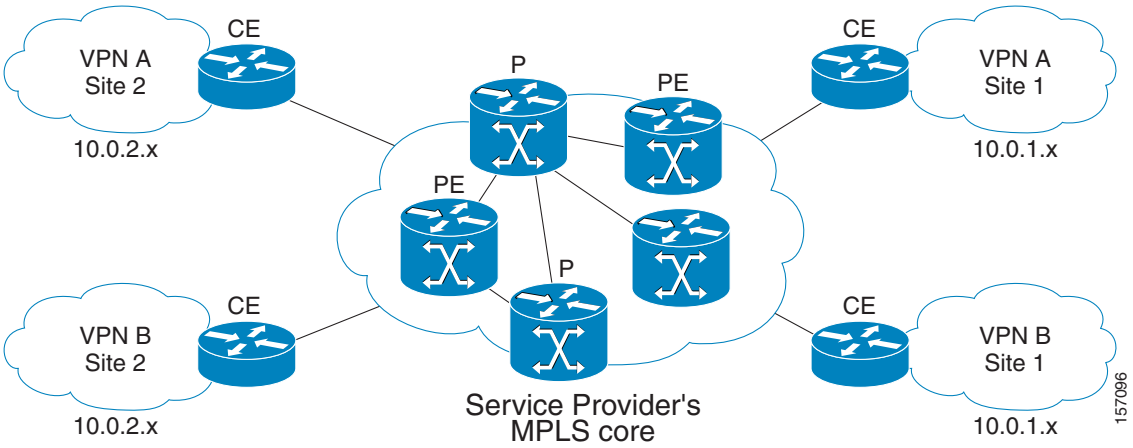
Customers that connect to the ISP using the VPN topology experience direct communication to the VPN sites as though they have their own private network even though their traffic is traversing a public network infrastructure and sharing the same infrastructure with other businesses.

Multiprotocol Label Switching (MPLS) is an emerging industry standard for implementing tag switching technology on high-speed routers in large IP networks. MPLS is designed to carry information of different protocols over a network and brings some of the advantages of circuit-switched networks to switched IP networks.

Connecting the MPLS protocol with VPN, the MPLS/VPN topology consists of a set of sites that are interconnected by means of an MPLS provider core network. At each site within the MPLS edge, one or more Customer Edge (CE) routers are attached to one or more Provider Edge (PE) routers. The Provider (P) router within the core routes packets to the PE routers. PE routers use the Border Gateway Protocol to communicate dynamically with each other.

Figure 27-1 illustrates the MPLS/VPN topology:

Figure 27-1 MPLS/VPN Topology



Some of the benefits of MPLS-based VPNs are seamless integration with customer intranets and increased scalability with numerous sites for each VPN and many VPNs for each service provider.

MPLS/VPN BGP LEG Overview

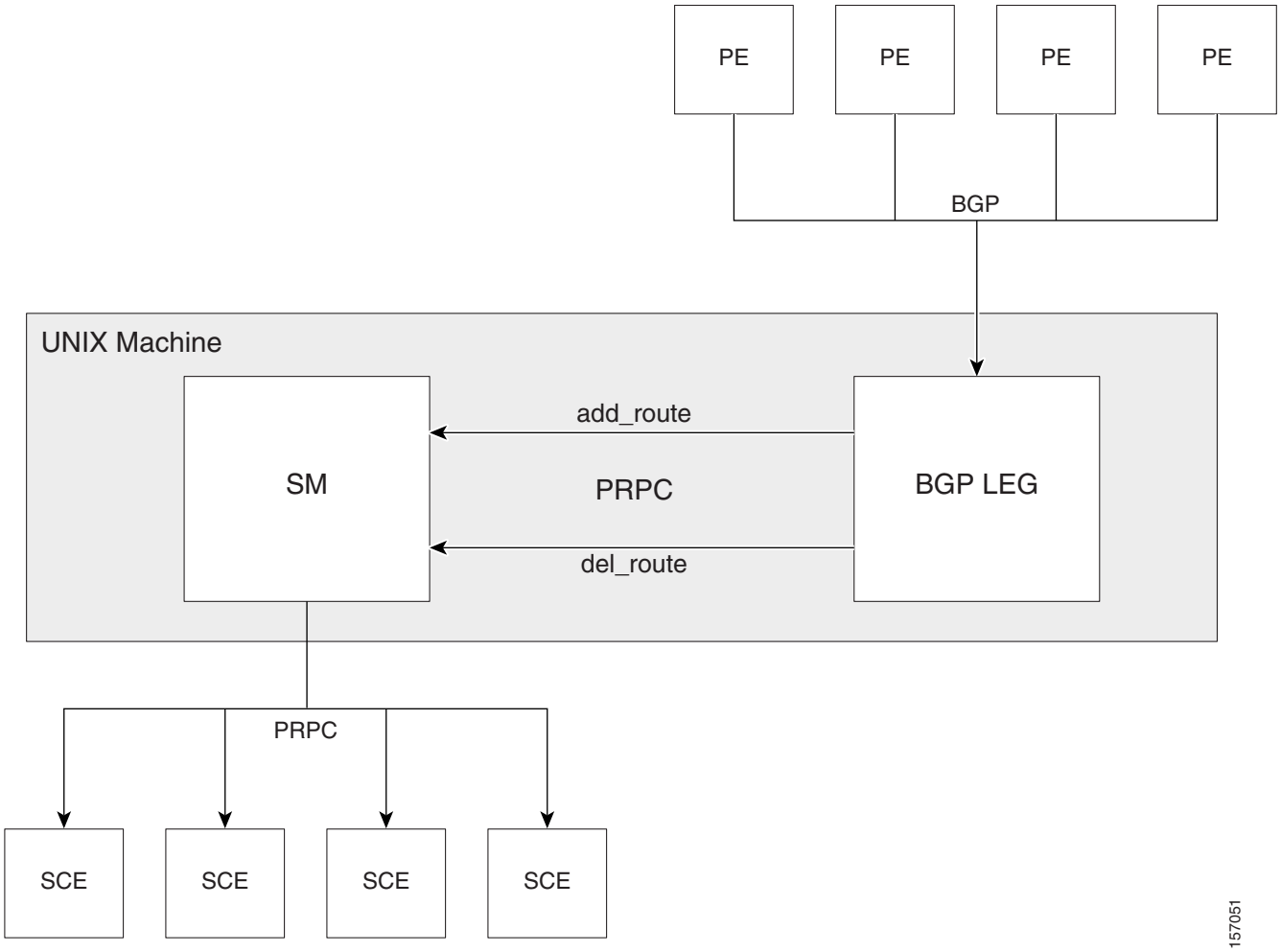
The MPLS/VPN BGP LEG solution consists of two components:

- BGP LEG—A UNIX daemon process that runs the BGP protocol to determine the BGP routes. This process runs under the root privileges.
- SM—The SM server stores subscriber and VPN information and updates the Service Control Engines (SCEs). The BGP adapter, an SM component, receives the routes from the BGP LEG and handles the adjustments to the regular VPN login/logout operations.

The SM and the BGP LEG are different processes that run on the same machine. The connection between the components is based on the PRPC protocol.

Figure 27-2 illustrates the MPLS/VPN BGP LEG solution:

Figure 27-2 MPLS/VPN BGP LEG Solution



The BGP LEG also supports receiving BGP updates from a Route Reflector (RR), instead of from each Provider Edge (PE) router separately. The BGP LEG can receive updates from a RR and from PEs that are not covered by the RR at the same time.

VPN Entity

A VPN entity is a group of VPN sites. The following parameters define a VPN site:

- The PE router that is connected to the VPN site. The IP address of the loopback interface identifies the router.
- An identifier for the VPN Virtual Routing and Forwarding (VRF) table. Either the Route Distinguisher (RD) of the VRF or the Route Target (RT) that is used for exporting or importing routes

The PE router assigns MPLS labels for each VPN site. The BGP protocol uses the MPLS labels to publish the VPN routes to the other PE routers. The BGP LEG listens to the BGP traffic, extracts the MPLS label, and adds the label to the VPN data in the SM database.

VPN Identifier (RD or RT)

The VPN can be identified using either the RD attribute or the RT attribute. It is necessary to decide which attribute best reflects the VPN partitioning, and then configure the SM accordingly. Note that the configuration is global for all the VPNs, that is all VPNs must be identified by the same attribute.

The RD is most commonly used to identify the distinct VPN routes of separate customers who connect to the provider. Therefore, in most cases the RD is a good partition for the VPNs in the network. Since the RD is an identifier of the local VRF, and not the target VRF, it can be used to distinguish between VPN sites that transfer information to a common central entity (for example, a central bank, IRS, Port Authority, and so forth).

The RT is used to define the destination VPN site. Although it is not intuitive to define the VPN based on its destination routes, it might be easier in some cases. For example, all when the VPN sites that communicate to a central bank are treated as a single VPN, it is worthwhile to use the RT as the VPN identifier.

It is important to note that the configuration is global. Thus, if at some point in time a certain VPN needs to be defined by RD, then all the VPN must be defined by RD as well. This is a point to consider when designing the initial deployment.

BGP LEG Scenario

The following scenario depicts the operation of the MPLS/VPN mode:

1. The SM starts up.
2. The BGP LEG establishes a PRPC connection to the SM.
3. The administrator imports the VPNs to the SM using a CSV file. The administrator specifies the following properties for each VPN:
   - VPN name
   - A list of VPN sites. Each VPN site is defined by:
   - VPN ID—The RD or RT that identifies the VPN's VRF
   - The IP address of the loopback interface of the PE router
   - SM domain
4. The administrator imports the VPN-based subscribers to the SM using another CSV file. The administrator specifies the following properties for each subscriber:
   - Subscriber name
   - A list of private IPs within the VPN using the syntax 'IP@VPN' (or a list of communities within a VPN as described in CE as Subscriber, page 27-5).
   - SM domain
   - A list of application properties. For example, the Service Control Application for Broadband (SCA BB) package ID, as described in the *Cisco Service Control Application for Broadband User Guide*.
5. The administrator configures the BGP LEG by specifying the PE routers that should be connected to it.
6. PE routers distribute routing information to the BGP LEG.

7. The BGP LEG analyzes BGP sessions and extracts the relevant data, such as RD/RT, MPLS label, and the loopback IP of the PE router.
8. The BGP LEG updates the VPN in the SM with the added or removed MPLS label.
9. The Subscriber Manager updates its database with the new VPN information and updates all of the SCE devices in the domain.

CE as Subscriber

An MPLS-VPN based subscriber can be defined to handle the traffic of a specific Customer Edge (CE) router. The BGP community field is used to correlate the private IP routes with the CE router. The subscriber is configured with a list of communities within the VPN using the syntax ‘community@VPN’.

When the BGP LEG analyzes the BGP session, it also extracts the community field, and adds all the IP routes in the BGP message to the subscriber that contains the same community field. This functionality takes place in addition to adding the VPN information to the SM as described in BGP LEG Scenario, page 27-4.