About the MPLS/VPN BGP LEG

This module describes the MPLS/VPN BGP LEG software module, and terms and concepts.
The SCMS SM MPLS/VPN BGP LEG is a software module that dynamically provides the MPLS label for each VPN using the BGP protocol. It listens to the BGP traffic to determine the correct MPLS label.

- MPLS/VPN Overview, page 1-1
- MPLS/VPN BGP LEG Overview, page 1-2
- Terms and Concepts, page 1-5

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 (BGP) to communicate dynamically with each other.

Figure 1-1 illustrates the 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.

- **Subscriber Manager (SM)**—The Subscriber Manager 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 1-2* illustrates the MPLS/VPN BGP LEG solution:
The BGP LEG also supports receiving BGP updates from a Route Reflector (RR), instead of from each PE router separately. The BGP LEG can receive updates from a Route Reflector and from PEs that are not covered by the Route Reflector at the same time.

VPN Entity

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

- The Provider Edge (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.
Chapter 1      About the MPLS/VPN BGP LEG

VPN Identifier (RD or RT)

The VPN can be identified using either the Route Distinguisher (RD) attribute or the Route Target (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, i.e. all VPNs must be identified by the same attribute.

The Route Distinguisher (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 (e.g. a central bank, IRS, Port Authority, etc.).

The Route Target (RT) is used to define the destination VPN site. Though it is not intuitive to define the VPN based on its destination routes, it might be easier in some cases. For example, if all the VPN sites that communicate to a central bank should be 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 Subscriber Manager starts up.
2. The BGP LEG establishes a PRPC connection to the Subscriber Manager.
3. The administrator imports the VPNs to the Subscriber Manager 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 Subscriber Manager 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 1-5).
   - 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 (SCA BB) 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 1-4.

**Terms and Concepts**

The following list of terms and concepts are necessary to understand the MPLS/VPN BGP LEG, configuration, and operation. Additional information regarding other issues can be found in the *Cisco Service Control Management Suite Subscriber Manager User Guide*.

- BGP (Border Gateway Protocol), page 1-6
- CE (Customer Edge), page 1-6
- LEG (Login Event Generator), page 1-6
- MPLS (Multi Protocol Label Switching), page 1-6
- PE (Provider Edge), page 1-6
- RD (Route Distinguisher), page 1-6
- RR (Route Reflector), page 1-6
- RT (Route Target), page 1-7
- Subscriber Domain, page 1-7
- Subscriber ID, page 1-7
- VPN ID, page 1-7
- Subscriber Mappings, page 1-7
- VPN (Virtual Private Networking), page 1-7
- VRF (Virtual Routing and Forwarding), page 1-7
BGP (Border Gateway Protocol)

An exterior gateway protocol used on the Internet to provide loop-free routing between different autonomous systems.
In the context of MPLS/VPN, the BGP protocol is used to distribute the MPLS/VPN routes of a PE router to its neighboring PE routers.

CE (Customer Edge)

A router on the service provider site that connects to the PE (Provider Edge), page 1-6 router in the MPLS core. The CE router only passes the message packet with the IP address and is not concerned with the MPLS/VPN label.

LEG (Login Event Generator)

A software component that performs subscriber login and logout operations on the SM, which is used to handle dynamic subscriber or VPN integration.

MPLS (Multi Protocol Label Switching)

A switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on pre-established IP routing information.

PE (Provider Edge)

A router in the service provider MPLS core that provides routing information between the customer router and the MPLS/VPN network. The PE router maintains a VRF (Virtual Routing and Forwarding), page 1-7 table for each customer site to determine how to route the packet.

RD (Route Distinguisher)

An 8-byte value that is concatenated with an IPv4 prefix to create a unique VPN IPv4 prefix. The RD uniquely identifies the VPN VRF within a PE router.

RR (Route Reflector)

A network element in the service provider network that is used to distribute BGP routes to the service provider BGP-enabled routers. Route Reflectors provide a mechanism for both minimizing the number of update messages transmitted within the autonomous system and reducing the amount of data that is propagated in each message.
Chapter 1  About the MPLS/VPN BGP LEG

Terms and Concepts

RT (Route Target)

Used by the routing protocols to control import and export policies and to build arbitrary VPN topologies for customers.

Subscriber Domain

The SM provides the option of partitioning SCE platforms and subscribers/VPNs into subscriber domains. A subscriber domain is a group of SCE platforms that share a group of subscribers/VPNs. Subscriber domains can be configured using the SM configuration file and can be viewed using the SM Command-Line Utility (CLU).

For additional information about domains and domain aliases, see the Cisco SCMS Subscriber Manager User Guide.

Subscriber ID

The Service Control solution requires a unique identifier for each subscriber. A subscriber ID represents a logical subscriber entity from the service provider perspective.

VPN ID

The Service Control solution requires a unique identifier for each VPN. A VPN ID represents a logical VPN entity from the service provider perspective.

Subscriber Mappings

The SCE platform requires mappings between the network IDs (IP addresses) of the flows it encounters and the subscriber IDs. The SM database contains the network IDs that map to the subscriber IDs. The SCE network-ID-to-subscriber mappings are constantly updated from the SM database.

VPN (Virtual Private Networking)

A technology for securely connecting a computer or network to a remote network over an intermediate network such as the Internet.

VPNs can use an insecure public network such as the Internet to connect two networks. They can also use an insecure public network to connect a network and a remote computer, or employ technologies such as tunneling, encryption, and authentication to secure the connection.

VRF (Virtual Routing and Forwarding)

In general, a VRF includes the routing information that defines the VPN site that is attached to a PE router. A VRF consists of an IP routing table, a forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table.