Cisco SCMS SM MPLS/VPN BGP LEG Reference Guide

Release 3.1
May 2007

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Customer Order Number:
Text Part Number: OL-8233-05

Cisco SCMS SM MPLS/VPN BGP LEG Reference Guide

CONTENTS

About this Guide

Revised: May 30, 2007, OL-8233-05

This guide describes the concept of a Multi Protocol Label Switching/Virtual Private Network (MPLS/VPN) architecture using the Login Event Generator (LEG) based on the Border Gateway Protocol (BGP), and explains how to install and configure it on the SCMS Subscriber Manager (SM) platform.

Note This guide assumes a basic familiarity with telecommunications equipment and installation procedures, Cisco SCMS subscriber management, subscriber integration concepts, and the MPLS/VPN architecture.

For complete information regarding Cisco's subscriber integration concept, see the *Cisco Service Control Management Suite Subscriber Manager (SCMS SM) User Guide* .

This introduction provides information about the following topics:

Audience

This document is intended for system administrators and system integrators who are familiar with the MPLS/VPN BGP LEG concepts and with Cisco Service Control Subscriber Management and Subscriber Integration concepts.

Document Revision History

Cisco Service Control Release	Part Number	Publication Date
Release 3.1.0	OL-8233-05	May, 2007

Description of Changes

- Updated for release 3.1.0.

Cisco Service Control Release	Part Number	Publication Date
Release 3.0.5	OL-8233-04	November, 2006

Description of Changes

- Updated for release 3.0.5.

Cisco Service Control Release	Part Number	Publication Date
Release 3.0.3	OL-8233-03	September, 2006

Description of Changes

- MPLS/VPN BGP LEG can be installed only on Red Hat Linux platforms.

Cisco Service Control Release	Part Number	Publication Date
Release 3.0.3	OL-8233-02	May, 2006

Description of Changes

- Added new section describing managing MPLS/VPN subscribers. See Managing MPLS/VPN Subscribers, page 1.
- Added new section describing the VPN identifier. See VPN Identifier (RD or RT), page 4.

Cisco Service Control Release	Part Number	Publication Date
Release 3.0	OL-8233-01	December, 2005

Description of Changes

- This is the first version of this document.

Organization

The major sections of this guide are as follows:

Table 1

Chapter	Title	Description
Chapter 1	About the MPLS/VPN BGP LEG, page 1	Describes the MPLS/VPN BGP LEG software module, and terms and concepts
Chapter 2	Installing the MPLS/VPN BGP LEG, page 1	Describes the installation process for installing the SM MPLS/VPN BGP LEG
Chapter 3	Configuring the MPLS/VPN BGP LEG, page 1	Provides the configuration instructions to configure the MPLS/VPN BGP LEG
Chapter 4	Managing MPLS/VPN Subscribers, page 1	Describes the management of MPLS/VPN subscribers
Chapter 5	Using the MPLS/VPN BGP LEG CLU, page 1	Describes the Command-Line Utility to control the operation of the MPLS/VPN BGP LEG and to retrieve information and statistics about the LEG

Related Publications

Use this *Cisco SCMS SM MPLS/VPN BGP LEG Reference Guide* in conjunction with the following Cisco documentation:

- *Cisco SCMS Subscriber Manager User Guide*
- *Cisco Service Control Application for Broadband User Guide*

Document Conventions

This guide uses the following conventions:

- **Bold** is used for commands, keywords, and buttons.
- *Italics* are used for command input for which you supply values.
- `Screen` font is used for examples of information that are displayed on the screen.
- **`Bold screen`** font is used for examples of information that you enter.
- Vertical bars (|) indicate separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate optional elements.
- Braces ({}) indicate a required choice.
- Braces within square brackets ([{}]) indicate a required choice within an optional element.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the guide.

Timesaver Means the *described action saves time*. You can save time by performing the action described in the paragraph.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warning **Means *danger*. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents. To see translated versions of warnings, refer to the *Regulatory Compliance and Safety Information* document that accompanied the device.**

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 1

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 subscriber using the BGP protocol. It listens to the BGP traffic to determine the correct MPLS label.

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.

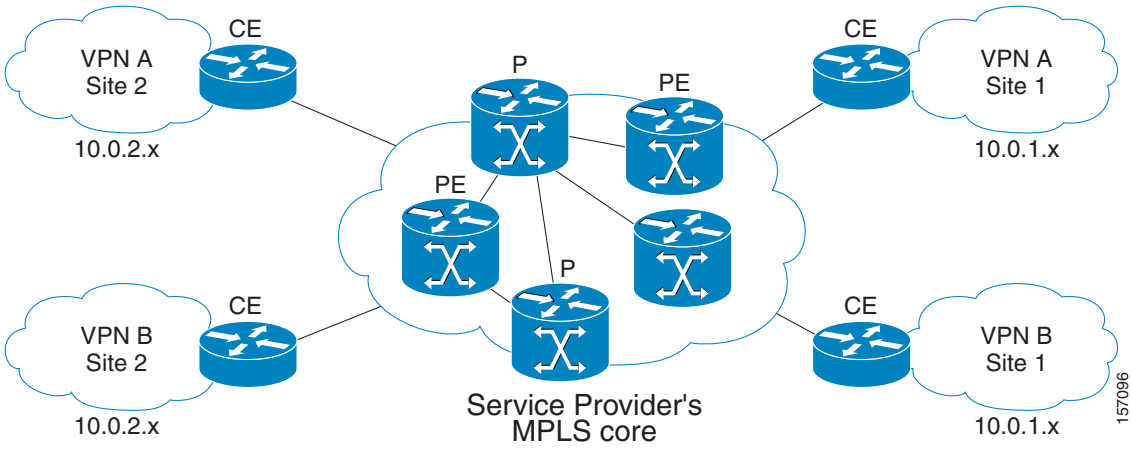
Customers that connect to the ISP using the VPN topology experience direct communication to the VPN sites as though they have their own private network even though their traffic is traversing a public network infrastructure and sharing the same infrastructure with other businesses.

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 on page 1-2 illustrates the MPLS/VPN topology.

Figure 1-1 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

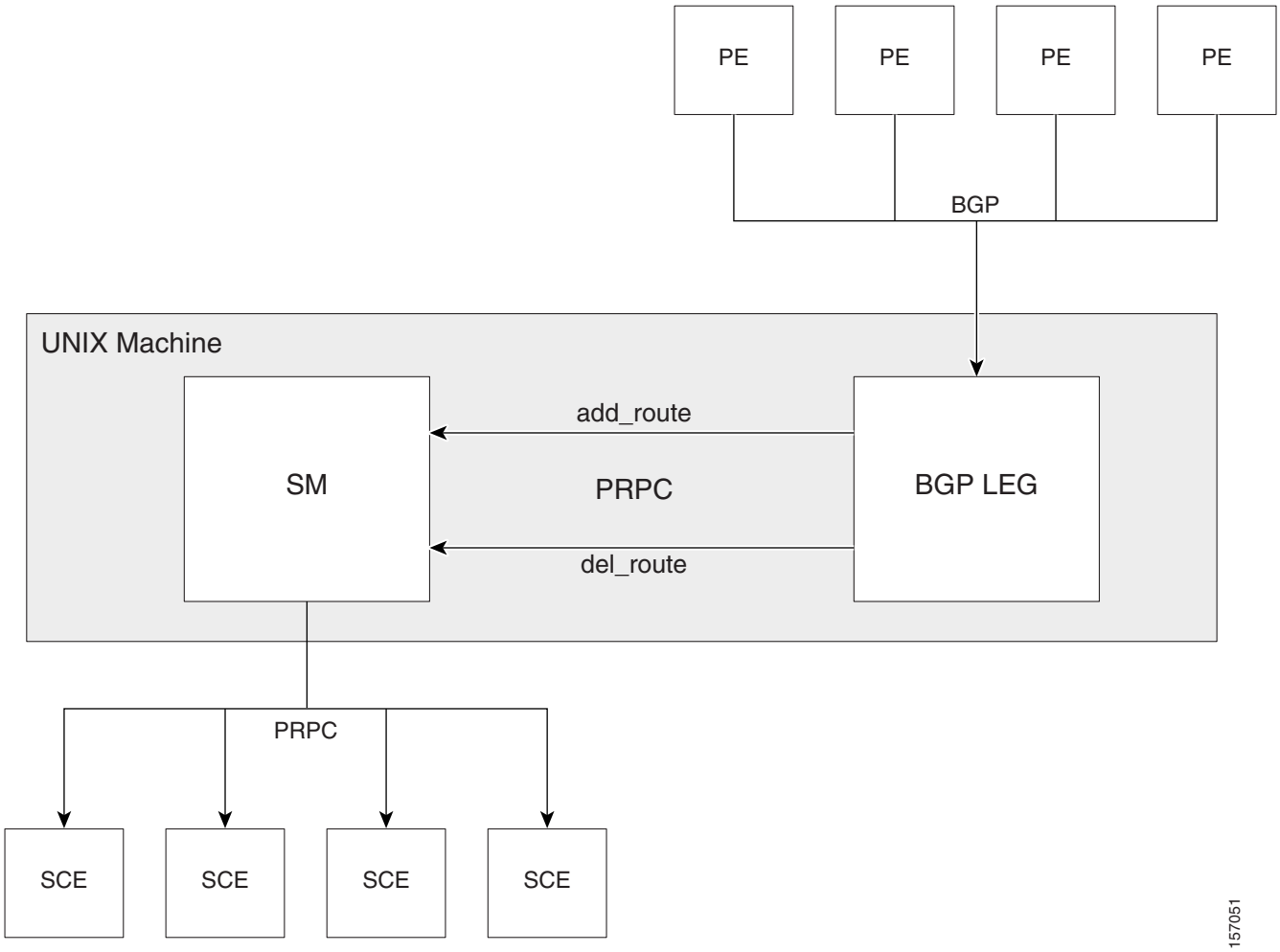
The MPLS/VPN BGP LEG solution consists of two components:

- BGP LEG—A UNIX daemon process that runs the BGP protocol to determine the BGP routes. This process runs under the root privileges.
- Subscriber Manager (SM)—The Subscriber Manager server stores subscriber 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 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 on page 1-3 illustrates the MPLS/VPN BGP LEG solution.

Figure 1-2 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 Subscriber

A VPN subscriber 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 subscriber data in the SM database.

VPN Identifier (RD or RT)

The VPN subscriber 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 subscriber partitioning, and then configure the SM accordingly. Note that the configuration is global for all the subscribers, i.e. all subscribers 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 subscribers 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 subscriber 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 subscriber, 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 subscriber needs to be defined by RD, then all the VPN subscribers 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 VPN subscribers to the Subscriber Manager using a CSV file. The administrator specifies the following properties for each VPN subscriber:
   - VPN subscriber name—Used as the subscriber 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
   - 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* .
4. The administrator configures the BGP LEG by specifying the PE routers that should be connected to it.
5. PE routers distribute routing information to the BGP LEG.
6. 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.
7. The BGP LEG updates the SM with the new information.
8. The Subscriber Manager updates its database with the new subscriber information and performs a login/logout operation to all of the SCE devices in the subscriber domain.

Note The MPLS/VPN BGP LEG automatically refreshes the BGP connections to all the relevant PEs after adding subscribers to the SM.

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)

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 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.

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 into subscriber domains. A subscriber domain is a group of SCE platforms that share a group of subscribers. 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.

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.

CHAPTER 2

Installing the MPLS/VPN BGP LEG

This module describes the installation process for installing and uninstalling the SM MPLS/VPN BGP LEG.

The SM MPLS/VPN BGP LEG is an external component that should be installed on the SM. The SM MPLS/VPN BGP LEG distribution is part of the SM LEG distribution.

The SM MPLS/VPN BGP LEG installation package includes a set of configuration files and the Command-Line Utility (CLU).

The SM MPLS/VPN BGP LEG can be installed only on Red Hat Linux platforms.

Package Contents

The following tables describes the contents of the SM MPLS/VPN BGP LEG distribution package supplied by Cisco:

Table 2-1 SM MPLS/VPN BGP LEG Distribution Package Contents

Path	File Name	Description
DIST_ROOT/bgp_leg		SM MPLS/VPN BGP LEG files
	bgp_leg.tar.gz	SM MPLS/VPN BGP LEG distribution
	Install	LEG installation procedure description
	install-bgp-leg.sh	SM MPLS/VPN BGP LEG installation script
	linux-def.sh	Linux specific definitions script
	sm-common.sh	General installation script

Installing the MPLS/VPN BGP LEG Software

SUMMARY STEPS

1. Copy the SM LEG distribution file to the SM machine and extract it with the **gunzip** command.
2. Run the BGP LEG installation script.
3. Add a VCS resource for the BGP LEG

DETAILED STEPS

Step 1 Copy the SM LEG distribution file to the SM machine and extract it with the **gunzip** command.

```
>gunzip SM_LEG_3.1.0_Bbbb.tar.gz >tar -xvf SM_LEG_3.1.0_Bbbb.tar.gz >cd bgp_leg
```

Step 2 Run the BGP LEG installation script.

```
#/install-bgp-leg.sh
```

The installation script automatically installs the SM MPLS/VPN BGP LEG on the SM and runs the OS specific definitions scripts according to your installation's operating system.

Note The installation script must run under root privileges.

Step 3 Add a VCS resource for the BGP LEG

Adding a VCS Resource to the BGP LEG

In a Subscriber Manager cluster topology, the Veritas Cluster Server (VCS) should monitor the BGP LEG process to verify that the process is running. To do so, you must configure the VCS with a resource that monitors and controls the LEG.

SUMMARY STEPS

1. Import the OnOnlyProcess agent's type from file:

   `/opt/VRTSvcs/bin/OnOnlyProcess/OnOnlyProcess.cf`

2. Add an OnOnlyProcess resource called "BGP_LEG" to the service group.
3. Run the **>ps -ea -o pid,s,args** command via telnet on each one of the servers.
4. Look for the line containing "bgpleg" in the text.
5. Define the **OnlineCmd**, **PathName**, and **Arguments** parameters:
6. Click **OK**.

DETAILED STEPS

Step 1 Import the OnOnlyProcess agent's type from file:

```
/opt/VRTSvcs/bin/OnOnlyProcess/OnOnlyProcess.cf
```

Step 2 Add an OnOnlyProcess resource called "BGP_LEG" to the service group.

Step 3 Run the **>ps -ea -o pid,s,args** command via telnet on each one of the servers.

Step 4 Look for the line containing "bgpleg" in the text.

This line contains the path and arguments of the BGP LEG to be used in the next step.

Step 5 Define the **OnlineCmd**, **PathName**, and **Arguments** parameters:

- **OnlineCmd**—Type the BGP LEG **start** command, for example:

  `/opt/pcube/sm/server/bin/p3bgp --start`

- **PathName**—Type the BGP LEG process path (from the previous step), for example:

  `/opt/pcube/sm/server/addons/bgpleg/bgpleg`

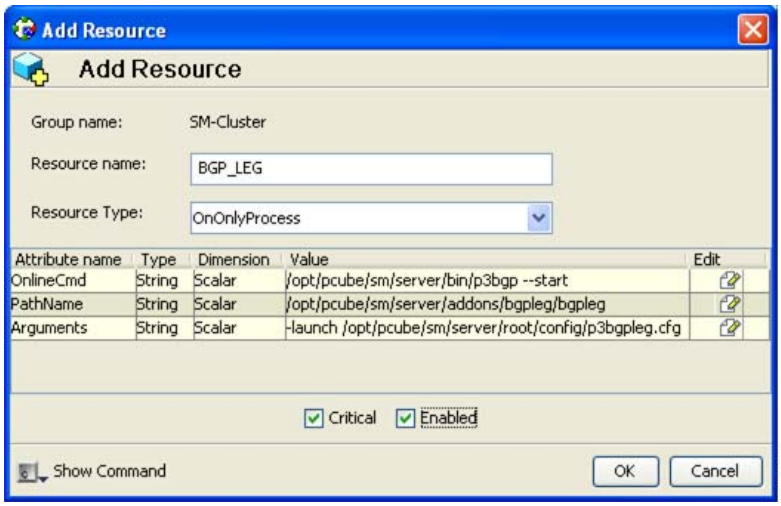
- **Arguments**—Type the BGP LEG process arguments (from the previous step). For example:

  `-launch /opt/pcube/sm/server/root/config/p3bgpleg.cfg`

Step 6 Click **OK**.

Figure 2-1 shows the Add Resource window.

Figure 2-1 Add VCS Resource Window



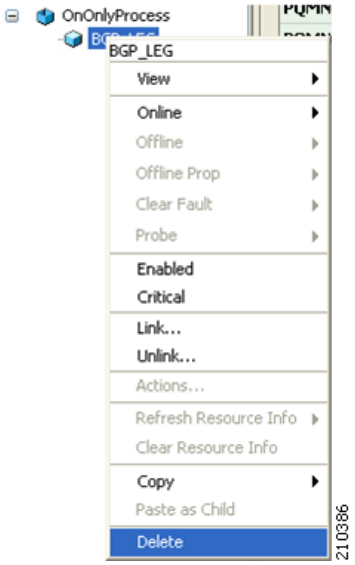
Note The arguments line might seem shorter than the actual full argument value, which is perfectly acceptable.

Removing a VCS Resource from the BGP LEG

Step 1 Right-click the BGP LEG resource icon you want to remove.

Step 2 From the drop-down list shown in Figure 2-2, choose **Delete**.

Figure 2-2 Removing a VCS Resource



Note The BGP LEG will be inactivated if there are no VCS resources. To activate the BGP LEG, there must be at least one resource.

CHAPTER 3

Configuring the MPLS/VPN BGP LEG

This module provides the configuration instructions to configure the MPLS/VPN BGP LEG

The SM MPLS/VPN BGP LEG is configured using the configuration file **p3bgpleg.cfg** file, which resides in the **sm-inst-dir/sm/server/root/config** directory (**sm-inst-dir** refers to the SM installation directory). The configuration file is loaded only upon the SM MPLS/VPN BGP LEG startup.

The configuration file holds the IP addresses of the PEs from which the routing information is gathered. When you reload the configuration file, all the BGP connections terminate and the BGP LEG waits for connections to be re-established from the IP addresses configured in the configuration file.

The configuration file consists of sections headed by a bracketed section title such as **[General]** for the general configuration section. Each section consists of one or more parameters having the format **parameter=value**. The number sign ("#") at the beginning of a line signifies that it is a comment.

Configuring the MPLS/VPN BGP LEG Settings

This section describes the configuration file settings for each section.

The **[General]** section contains the following parameters:

- `as-num`

  Defines the autonomous system number of the BGP LEG. This parameter is mandatory and has no default value.

  Possible values are 1 to 65535.

- `max-route-burst`

  Defines an estimation of the expected burst of routes upon PE connection/refresh-all.

  This parameter sets the PRPC buffer size between the BGP LEG and the SM.

  The parameter is mandatory and has a default value of 100,000 routes in the p3bgpcfg configuration file.

The **[PE.xxxxxxxx]** section holds the PE or Route Reflector information. Each PE section must include a unique PE/Route Reflector name. The section contains the following parameters:

- `access`

Defines the IP address or addresses that the PE/Route Reflector accesses (in dotted notation). It is mandatory to configure at least one access IP address. Additional IP addresses, if needed, should be on the same line, separated by comma. The same IP address cannot appear in two PE sections.

- `as-num`

  Defines the autonomous system number connected to the PE/Route Reflector. This parameter is not required. If not specified, the as-num defined in the **[General]** section is used.

Configuration File Example

The following example illustrates the MPLS/VPN BGP LEG configuration file:

```
[General]
as-num=255
max-route-burst=100000
[PE.site104]
access=10.56.211.80, 10.0.1.2, 10.55.123.56
[PE.site110]
access=10.28.233.129
as-num=110
[PE.10.56.211.81]
access=10.56.211.81
```

Configuring the SM for the MPLS/VPN BGP LEG

You must configure the Subscriber Manager to support the SM MPLS/VPN BGP LEG. The SM configuration file, **p3sm.cfg** contains a configuration section for MPLS/VPN called **[MPLS/VPN]**. The section contains the following parameters:

- `vpn_id`

  Defines the BGP attribute that is used to identify the VPN subscribers.

  Possible values for this parameter are **RD**and **RT**.

  The default value is **RT**.

- `log_all`

  Defines the logging level of the BGP LEG.

  Possible values for this parameter are **true**or **false**.

  The default value is **false**.

  If this parameter is set to **true**, the SM logs all received BGP packets. Set this parameter to true during the integration/testing phase.

For further information on configuring the SM, see the *Cisco SCMS Subscriber Manager User Guide* .

CHAPTER 4

Managing MPLS/VPN Subscribers

This module describes how to manage MPLS/VPN subscribers.

You use a set of Command-Line Utilities (CLU) to control the SM. The **p3subs** is the CLU that manages the SM subscribers. A detailed description of the SM CLU can be found in the *Cisco SCMS Subscriber Manager User Guide* .

This module covers the information relevant for MPLS/VPN subscribers.

Adding MPLS/VPN Subscribers

Adding MPLS/VPN Subscribers

A set of [VPN-ID, PE-IP] pairs defines each subscriber. The VPN-ID is the RD or RT that identifies the subscriber, and the PE-IP is the loopback IP address of the PE router that is connected to the VPN site.

Note You must add MPLS/VPN subscribers to the SM before starting the BGP LEG. Otherwise, the BGP labels of the subscribers will not be added to the SM, and you will have to send a route refresh request to the PE.

Note To add multiple MPLS/VPN subscribers, prepare a CSV file containing the subscriber information, and use the CLU **p3subsdb --import**. The network-ID of the MPLS/VPN subscribers is VPN-ID@PE-IP, as described previously.

Step 1 From the shell prompt, use the **p3subs --add** command.

The command should be of the following general format:

```
p3subs--add--subscriber=Subscriber-name[--mpls-vpn=VPN-ID@PE-IP[,MORE]]
[--property=property-name=value] [--domain=domain-name]
```

Adding VPN Sites to Existing Subscribers

The **p3subs --set** operation adds a VPN site (identified by the VPN-ID) behind the PE router (whose IP address is PE-IP) to an existing subscriber.

Step 1 From the shell prompt, use the **p3subs --set**command.

The command should be of the following general format:

```
p3subs--set--subscriber=Subscriber-name[--mpls-vpn=VPN-ID@PE-IP]
```

Displaying an MPLS/VPN Subscriber

Step 1 From the shell prompt, use the **p3subs --show command**.

The command should be of the following general format:

```
p3subs--show--subscriber=Subscriber-name
```

This operation has the following output:

```
Name:VPN1
Domain:  subscribers
Mappings:
MPLS/VPN: 1:1000@1.1.1.1(no BGP information)
MPLS/VPN: 1:1001@1.1.1.1label: 10 IP range: 10.1.1.1/24
```

According to this output, the subscriber VPN1 has two VPN sites: 1:1000 and 1:1001. Both sites are behind the same PE whose IP address is 1.1.1.1. The VPN site 1:1000 did not receive any BGP routes. The VPN site 1:1001 received one BGP route with the label 10 corresponding to the subnet 10.1.1.1/24.

Removing MPLS/VPN Subscribers

Removing an MPLS/VPN Subscriber

The **p3subs --remove** operation can be used to remove an entire subscriber from the SM including the entire VPN site and any received BGP updates.

Step 1 From the shell prompt, use the **p3subs --remove** command.

The command should be of the following general format:

```
p3subs--remove--subscriber=Subscriber-name
```

Removing a VPN Site from a Subscriber

The **p3subs --remove**operation can be used to remove a VPN site (identified by VPN-ID) behind the PE router (whose IP address is PE-IP)from a specific subscriber 'Subscriber-Name'. It also removes all the BGP routes that were received for this VPN site.

Step 1 From the shell prompt, use the **p3subs --remove**command.

The command should be of the following general format:

```
p3subs--remove--subscriber=Subscriber-name--mpls-vpn=VPN-ID@PE-IP
```

Removing all MPLS/VPN Subscribers

Step 1 From the shell prompt, use the **p3subs --remove-all-mpls-vpn**command.

This command removes all MPLS/VPN subscribers.

CHAPTER 5

Using the MPLS/VPN BGP LEG CLU

This module describes the MPLS/VPN BGP LEG CLU.

Information About the MPLS/VPN BGP LEG CLU

The p3bgp utility controls the operation of the BGP LEG and displays its status. The command format is the following:

```
p3bgp <operation>[parameter]
```

Table 5-1 lists the **p3bgp** operations:

Table 5-1 p3bgp Operations

Operation	Description
--start	Starts the BGP LEG
--stop	Stops the BGP LEG
--restart	Restarts the BGP LEG
--status	Displays a short status line for each PE/RR
--show	Displays a detailed status for a specific PE/RR
--show-all	Displays a detailed status for each PE/RR
--refresh	Sends a refresh request to specific PE/RR to receive updated information on all routes
--refresh-all	Sends a refresh request to all PE/RR to receive updated information on all routes. Use this operation when the PE/RR is disconnected from the LEG and you want to make sure that all the BGP information is propagated to the SCE boxes. The refresh is for new information only; obsolete labels are not checked for validity.

Table 5-1 p3bgp Operations

Operation	Description
--force-sync	Used together with **--refresh-all**. Sends a refresh request to all PE/RR to receive updated information on all routes, and then synchronizes this information with all SCE boxes. After this operation is completed, the SCE boxes are updated with the BGP information. Use this operation when the PE/RR is disconnected from the LEG and you want to make sure that all the BGP information is propagated to the SCE boxes. This operation also makes sure that obsolete labels are removed from the SCE boxes.
--load-config	Loads the configuration file to the BGP LEG. This operation also restarts the BGP LEG.
--help	Displays the available **p3bgp**commands

BGP LEG Status

The following is an example of the **p3bgp** command-line utility using the status operation:

ID	Peer IP	PE Name	Updates recv	Notify recv	K.Alive sent	K.Alive recv	Hold Time
1	1.2.3.4	PE101	150	0	58	57	157
2	1.2.3.5	PE102	183	0	34	33	77

The following list is a description of the status operation output:

- Peer IP—The IP of the PE/RR that is connected to the LEG
- PE name—The name of the PE/RR as configured in the configuration file
- Updates recv—A counter for all the BGP updates received from this PE/RR
- Notify recv—A counter for all the BGP notifications received from this PE/RR
- K.Alive sent—A counter for all the BGP keep alives sent to this PE/RR
- K.Alive recv—A counter for all the BGP keep alives received from this PE/RR
- Hold Time—The remaining time-out for the next keep alive

BGP LEG Detailed Status

The following is an example of the **p3bgp**command line utility using the **show**operation on a specific PE router named PE101:

```
1 : PE101
connects                    : 1
recv UPDATE                 : 150
recv KEEPALIVE              : 57
sent KEEPALIVE              : 58
recv NOTIFY                 : 0
current holdtime            : 157
TCP sndwnd                  : 16384
TCP rcvwnd                  : 87380
Connection up time          : 0 Days, 1 Hrs, 7 Min, 59 Sec
refresh requests            : 2
recv PE AddRoute messages   : 2
send SM AddRoute messages   : 10
send SM not connected       : 0
BGP state                   : Established
```

The following list is a description of the show operation output:

- connects—The number of successful connections established with this PE/RR since the LEG is up.
- recv UPDATE—A counter for all the BGP updates received from this PE/RR
- recv KEEPALIVE—A counter for all the BGP keep alives received from this PE/RR
- sent KEEPALIVE—A counter for all the BGP keep alives sent to this PE/RR
- recv NOTIFY—A counter for all the BGP notifications received from this PE/RR
- current holdtime—The remaining time-out for the next keep alive
- TCP sndwnd—The TCP send window buffer size
- TCP rcvwnd—The TCP receive window size
- Connection up time—The time since the connection to this PE/RR was established
- refresh requests—A counter for the number of refresh requests requested for this PE/RR
- recv PE AddRoute messages—A counter for BGP add-route messages received from the PE/RR
- send SM AddRoute message—A counter for successful add routes invocations performed on the SM for this PE/RR
- send SM not connected—A counter for SM invocations that were kept in an internal buffer due to disconnected SM
- BGP state—The state of the BGP connection to this PE/RR