Cisco SCMS SM MPLS/VPN BGP LEG

Reference Guide

Version 3.0.3
OL-8233-03

Corporate 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: 408 526-4100

Customer Order Number: DOC-8233-03=
Text Part Number: OL-8233-03

Printed in the USA on recycled paper containing 10% postconsumer waste.

Cisco SM MPLS/VPN BGP LEG Reference Guide

CONTENTS

Preface

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 *Service Control Management Suite Subscriber Manager (SCMS SM) User Guide.*

Document Revision History

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

Description of Changes

- Added support for Red Hat Linux platforms

Cisco Service Center 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* (on page 4-1).
- Added new section describing the VPN identifier. See *VPN Identifier (RD or RT)* (on page 1-4).
- Various other small changes to text.

Release 3.0	OL-8233-01	December, 2005

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.

Organization

This guide covers the following topics:

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

Related Documentation

This Reference Guide should be used in conjunction with the following Cisco documentation:

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

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{x | y | z}	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Convention	Description
string	A nonquoted set of characters. Do not use quotation marks around the string, or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
`italic screen` font	Arguments for which you supply values are in *`italic screen`* font.
→	This pointer highlights an important line of text in an example.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Cautions use the following conventions:

Caution Means *reader be careful*. You are capable of doing something that might result in equipment damage or loss of data.

Warnings use the following conventions:

Warning Means *reader be warned*. You are capable of doing something that might result in bodily injury.

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- *http://www.cisco.com*

- *http://www-china.cisco.com*
- *http://www-europe.cisco.com*

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/pcgi-bin/marketplace/welcome.pl

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can email your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides *Cisco.com* (on page vii) as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for *Cisco.com* (on page vii), go to the following website:

http://tools.cisco.com/RPF/register/register.do

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

About the MPLS/VPN BGP LEG

The ***Cisco 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.

This chapter contains the following sections:

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.

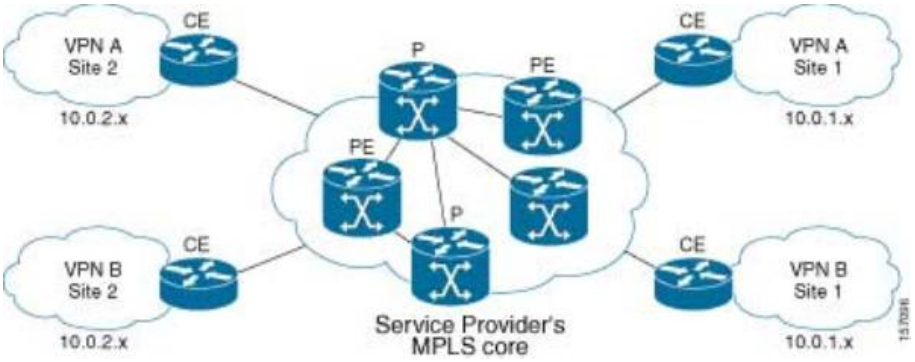
Customers that connect to the ISP using the VPN topology experience direct communication to the VPN sites as though they have their own private network even though their traffic is traversing a public network infrastructure and sharing the same infrastructure with other businesses.

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 dynamically communicate with each other.

The following diagram 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

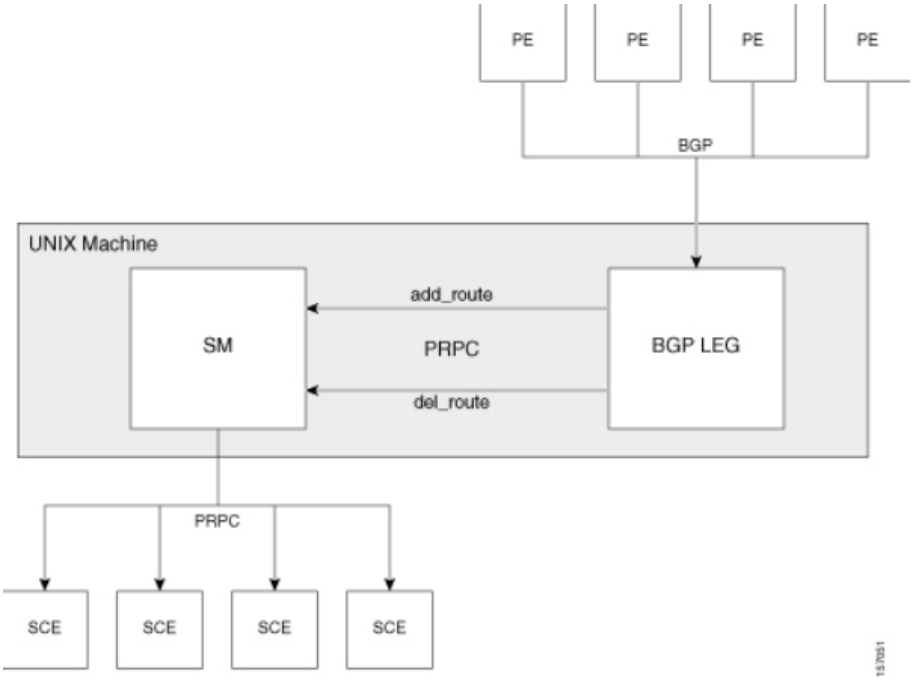
The MPLS/VPN BGP LEG solution is divided into 2 components:

- 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.

The following diagram 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 which are not covered by the Route Reflector at the same time.

VPN Subscriber

A VPN subscriber is a group of VPN sites. A VPN site is defined by the following parameters:

- The Provider Edge (PE) router that is connected to the VPN site. The router is identified by the IP address of the loopback interface.
- An identifier for the VPN Virtual Routing and Forwarding (VRF) table – 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 MPLS labels are used by the BGP protocol 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:

Step 1 The Subscriber Manager starts up.

Step 2 BGP LEG establishes a PRPC connection to the Subscriber Manager.

Step 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:

a) VPN subscriber name—used as the subscriber name

b) 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

c) SM domain

d) A list of application properties. For example, the Service Control Application for Broadband (SCA BB) package ID, as described in the SCA BB User Guide

Step 4 The administrator configures the BGP LEG by specifying the PE routers that should be connected to it.

Step 5 PE routers distribute routing information to the BGP LEG.

Step 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.

Step 7 The BGP LEG updates the SM with the new information.

Step 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 SM 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 *Service Control Management Suite Subscriber Manager (SCMS SM) 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)* (on page 1-5) 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 preestablished 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)* (on page 1-7) table for each customer site to determine how the packet is to be routed.

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 *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 or 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.

Installing the MPLS/VPN BGP LEG

This chapter describes the procedures for installing the SM MPLS/VPN BGP LEG software module. It also describes the uninstall procedure.

The SM MPLS/VPN BGP LEG is provided as 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.

This chapter contains the following sections:

Package Contents

The contents of the SM MPLS/VPN BGP LEG distribution package supplied by Cisco are described in the following table:

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

To install the SM MPLS/VPN BGP LEG on the SM machine:

Step 1 Copy the SM LEG distribution file to the SM machine and extract it by performing the following operation:

```
> gunzip SM_LEG_3.0.3 Bbbb.tar.gz
> tar –xvf SM_LEG_3.0.3_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.

Step 3 Add a VCS resource for the BGP LEG (optional for cluster setups)

Note The installation script must run under root privileges.

Adding a VCS Resource to the BGP LEG

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

To add a BGP LEG resource:

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 following command via telnet session on each one of the servers:

>ps -ea -o pid,s,args

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 following parameters:

a) OnlineCmd—Type the BGP LEG start command, for example:

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

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

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

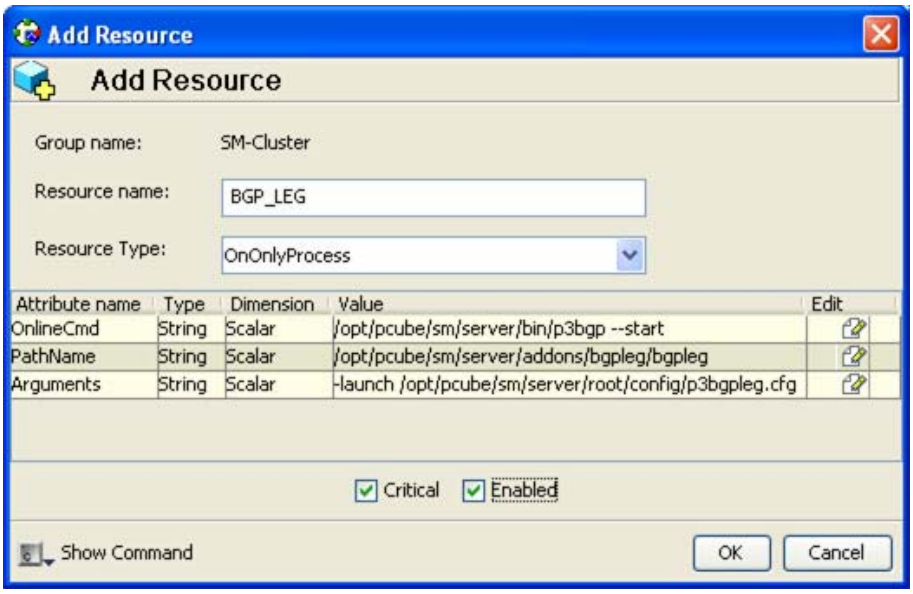
c) Arguments—Type the BGP LEG process arguments (from the previous step). For example:

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

Step 6 Click **OK**.

The following figure displays 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.

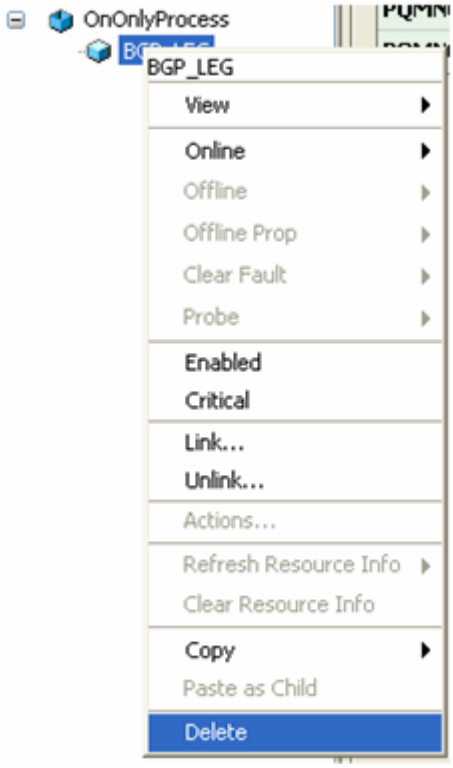
Removing a VCS Resource from the BGP LEG

To remove a VCS resource from the BGP LEG:

Step 1 Right-click the BGP LEG resource icon to be removed.

Step 2 From the drop-down list, 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 chapter explains how to configure the SM 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 the configuration file is reloaded, all 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 is made up 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.

This chapter contains the following sections:

Configuring the MPLS/VPN BGP LEG Settings

This section describes the configuration file settings for each section.

The `[General]` section contains the following parameter:

- *`as-num`*

  Defines the autonomous system number of the BGP LEG. This parameter is mandatory and has no default value.
  Possible values are 1 - 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 100K 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

The Subscriber Manager must be configured 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: RD or RT. The default value is RT.

- *log_all*

  Defines the logging level of the BGP LEG. Possible values: true or false. The default value is false. If set to true, the SM logs all BGP packets that were received by it. Use it during integration/testing phase.

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

Managing MPLS/VPN Subscribers

This chapter explains how to manage MPLS/VPN subscribers.

The SM is controlled by a set of command line utilities (CLU). The p3subs is the CLU that is used to manage the SM subscribers. A detailed description of the SM CLU can be found in the *SCMS Subscriber Manager User Guide*.

This chapter covers the relevant information that is used for MPLS/VPN subscribers.

This chapter contains the following sections:

Adding MPLS/VPN Subscribers

To add an MPLS/VPN subscriber, use the following CLU:

From the shell prompt, enter a command using the following general format:

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

Each subscriber is defined by a set of [VPN-ID, PE-IP] pairs. 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 MPLS/VPN subscribers must be added to the SM before the BGP LEG is started. 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 above.

To add a VPN site to an existing subscriber, use the following CLU:

From the shell prompt, enter a command using the following general format:

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

This operation adds the VPN site (identified by the VPN-ID) behind the PE router (whose IP address is PE-IP) to the existing subscriber 'Subscriber-Name'.

Displaying MPLS/VPN Subscribers

To display an MPLS/VPN subscriber, use the following CLU:

From the shell prompt, enter a command using 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@1.1.1.1  label: 10 IP range: 10.1.1.1/24
```

According to this output, the subscriber VPN1 has 2 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

To remove an MPLS/VPN subscriber, use the following CLU:

From the shell prompt, enter a command using the following general format:

p3subs --*remove* **--subscriber=***Subscriber-name*

This operation removes the entire subscriber from the SM including the entire VPN site and the BGP updates that were received for it.

To remove a VPN site from a subscriber, use the following CLU:

From the shell prompt, enter a command using the following general format:

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

This operation removes the VPN site (identified by VPN-ID) behind the PE router (whose IP address is PE-IP) from the subscriber 'Subscriber-Name'. All the BGP routes that were received for this VPN site are also removed.

Removing all MPLS/VPN Subscribers

To remove all MPLS/VPN subscribers, use the following CLU:

From the shell prompt, enter a command using the following general format:

p3subsdb --*remove-all-mpls-vpn*

MPLS/VPN BGP LEG Command-Line Utility (CLU)

This chapter contains the following sections:

p3bgp Utility

The **p3bgp** utility is used to control the operation of the BGP LEG and to view its status.

The command format is:

p3bgp **`operation`** [**`parameter`**]

The following table 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. This operation should be used when the PE/RR was 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.

--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. This operation should be used when the PE/RR was 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     PE     Updates  Notify   K.Alive  K.Alive  Hold
     IP       Name   recv     recv     sent     recv     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

Index

T

V