CHAPTER 13

MPLS/VPN Support

Revised: June 27, 2011, OL-21098-07

Introduction

This chapter provides an overview of the Service Control MPLS/VPN support. It also explains the various procedures for configuring and monitoring MPLS/VPN.

Service Control in the MPLS/VPN Environment

MPLS/VPN networks are very complex and utilize many routing protocols and many different levels of addressing and control. In addition, the various VPNs may use overlapping IP addresses (private IPs).

The SCE platform makes a distinction between identical IP addresses that come from different VPNs, and maps them into subscribers according to the MPLS labels attached to the packets. This involves various mechanisms in all levels of the system.

The following assumptions and requirements allow the SCE platform to operate in an MPLS/VPN environment:

- The MPLS/VPN architecture is according to RFC-2547.
- The specific type of encapsulation used is the MPLS shim header over Ethernet (described in RFC-3032).

- There are two levels of MPLS labels.
  - External labels — Used for transport over the service provider MPLS core network.

  These labels are not mandatory for VPN classification, and some situations do not appear in the packet due to PHP or other reasons.
  - Internal labels (BGP labels) — Used to identify the VPNs connected to each edge router, and typically controlled by the BGP protocol.

  These labels are mandatory for VPN classification.
- The MPLS/VPN solution contains the SCE platform and the SM. The SM acts as a BGP peer for the PE routers in the service provider network, and communicates the BGP information to the SCE platform as subscriber information.

Note The MPLS/VPN solution supports the existence of non-VPN-based subscribers concurrently with the MPLS/VPN-based subscribers (see Non-VPN-Based Subscribers, page 13-6).

Definitions and Acronyms

Table 13-1 defines important terms and acronyms.

Table 13-1 MPLS/VPN Terms and Acronyms

Term or Acronym	Definition
PE (Provider Edge router)	A router at the edge of the service provider network. The PE routers are the ones that connect to the customers, and maintain the VPNs
P (Provider router)	A router in the core of the service provider network. P routers only forward MPLS packets, regardless of VPNs.
VPN (Virtual Private Network)	In the Service Control context, a VPN is the part of the VPN that resides in a specific site. It is a managed entity over which private IP subscribers can be managed.
BGP LEG	A software module that resides on the SM server and generates BGP-related login events. The BGP LEG communicates with the BGP routers (PEs) and passes the relevant updates to the SM software, which generates login events to the SCE platform for the updated VPN-based subscribers.
Upstream	Traffic coming from the PE router and going into the P router
Downstream	Traffic coming from the P router and going into the PE router
RD (Route Distinguisher)	Used to uniquely identify the same network/mask from different VRFs (such as, 10.0.0.0/8 from VPN A and 10.0.0.0/8 from VPN B)
RT (Route Target)	Used by the routing protocols to control import and export policies, to build arbitrary VPN topologies for customers
VRF (Virtual Routing and Forwarding instance)	Mechanism used to build per-interface routing tables. Each PE has several VRFs, one for each site it connects to. This is how the private IPs remain unique.

What are the Challenges for Service Control for MPLS/VPN Support?

- Private IP addresses cause flows to look the same except for their MPLS labels.
- The MPLS labels are different in each direction, and must be matched.
- Detecting that a flow belongs to a certain VPN is complicated by the fact that in the downstream direction there is no external label. The SCE platform must be able to understand the VPN information from the internal label + the MAC address of the PE.

How MPLS/VPN Support Works

Service Control supports three mechanisms that make MPLS/VPN support work:

- Flow detection – This is the job of the SCE platform, to match upstream and downstream traffic to identify flows.
- VPN detection – Downstream VPN labels are identified by the SM. The SCE platform learns the upstream labels from the traffic to identify the VPN.
- Subscriber detection – The SM and the SCE platform function together to identify the IP range within a VPN that is defined as a single subscriber.

Flow Detection

Flow detection is the process of deciding which packets belong to the same flow. This relates to the first two challenges listed:

- Private IP addresses cause flows to look the same except for their MPLS labels.
- The MPLS labels are different in each direction, and must be matched.

Flow detection is based on the MPLS labels, extending the basic 5 tuple that SCOS uses to identify flows, and taking into account the fact that in MPLS, the packet is labeled differently in each direction.

Since MPLS traffic is unidirectional, each direction is classified separately by the SCE platform, using the following:

- Downstream – the BGP label and the MAC address of the PE (only one label that is relevant to the classification)

  Downstream labels are learned from the control plane (through the SM BGP LEG).
- Upstream – the combination of the external label, the BGP label, and the MAC address of the P router (two labels that are relevant to the classification)

  Upstream labels are learned from the data plane.

VPN Detection

The network configuration that provides the division into VPNs is controlled by the SM. The network-wide value that describes a VPN most closely is either the Route Target or the Route Distinguisher

- The administrator configures the SM to detect VPNs, according to selected attribute (RT or RD).
- The network operator provides the SCE platform with a mapping between RT values and VPN subscriber names.

The relevant module in the Subscriber Manager server (SM) is the BGP-LEG. The BGP-LEG is added to the BGP neighborhood for obtaining the information on the MPLS labels. The local PEs are configured to add the BGP-LEG as a BGP peer.

The SCE platform detects that a flow belongs to a certain VPN according to the downstream label that the flow carries, and the MAC address of the PE that it is sent to.

One VPN may spread over more than one PE router, as long as all the sites of the VPN are connected to the subscriber side of the same SCE platform

VPNs can be configured only via the SM. The SCE platform CLI can be used to view VPN-related information, but not to configure the VPNs.

Subscriber Detection

What is an MPLS/VPN-based Subscriber?

As in other modes of operation, in MPLS/VPN each flow belongs to a certain subscriber. A VPN-based subscriber is a part of a VPN. The VPN itself corresponds to a set of IP addresses that are managed separately and that belong to a specific ISP customer who pays for the VPN service.

An MPLS/VPN-based subscriber can be defined as either of the following:

- A set of IP addresses or ranges in a certain VPN.
- All the IP addresses of a CE router, defined by a BGP community over a VPN.

The network configuration that provides the division into VPNs and VPN-based subscribers is controlled by the SM. (For more information, see the *Cisco Service Control Management Suite Subscriber Manager User Guide*.)

Private IP Subscriber Support

VPN-based subscribers can have private IP mappings, which are a combination of an IP range and a VPN mapping. Since the source of such mappings is typically in the BGP protocol, and they are received automatically from the protocol by the BGP agent, the IP ranges may contain overlapping ranges. The semantics of such overlaps is that of a longest prefix match.

For example, if subscriber A receives the range 10.0.0.0/8@VPN1 and subscriber B receives the range 10.1.0.0/16@VPN1, then the system maps IPs that start with 10.1 to subscriber B, and any other address that begins with 10 to subscriber A. Traffic with other IP addresses on VPN1 will be mapped to the unknown subscriber.

For private IP subscribers, flows are distributed to traffic processors according to the VPN, not according to the IP address. This means that all traffic from any one VPN is mapped to the same traffic processor.

How the Service Control MPLS/VPN Solution Works

How the Service Control MPLS/VPN Solution Works: A Summary

- The SM is configured with the VPNs and VPN-based subscribers that should be managed.

  A VPN is identified by the RD / RT and the PE.
- The BGP-LEG updates the SM with the MPLS labels and IP routes.
- The SM pushes the VPNs with their labels and the VPN-based subscriber to the SCE platform with the downstream MPLS labels of the VPN.
- The SCE platform resolves the PE MAC addresses and updates its tables with the new information.
- The SCE platform learns the upstream labels, including the P MAC address.
- The SCE platform provides the regular services to the VPN-based subscribers (BW management, reports, etc.)

SCE Platform Tasks in the MPLS/VPN Solution

- Matching upstream to downstream labels
  - Mappings of downstream labels to VPNs are received from the SM
  - Upstream labels are learned from the data
- The MAC addresses of the PEs are used to distinguish downstream labels of different PEs
- After the learning, each flow is classified as belonging to one of the VPNs.
- The SCE platform performs a longest prefix match on the IP address inside the VPN, and classifies each flow to the correct VPN-based subscriber
- The SCE platform runs the SCA-BB application for the network flows, which are classified to VPNs, thus providing subscriber aware service control and reporting

BGP LEG Tasks in the MPLS/VPN Solution

- The BGP LEG is a software module that runs on the SM server
- The LEG maintains a BGP session with a list of PEs
- After the sessions establishment, the LEG propagates MP-BGP route-updates from the PEs to the SM module

SM Tasks in the MPLS/VPN Solution

- The VPNs are stored in the SM database.
- Each VPN is defined by:
  - The IP address of the loopback interface of the PE router.
  - The RD or RT that identifies the VPN within the PE router.
- A VPN-based subscriber is defined by the IP range in a specified VPN or the BGP community (CE as subscriber).
- The SM receives updates from the BGP LEG, and updates the VPN information with the new MPLS labels.
- The relevant SCE platforms that will get the MPLS updates are defined by the VPN domain.

Service Control MPLS/VPN Concepts

Non-VPN-Based Subscribers

The MPLS/VPN solution supports the existence of non-VPN-based (regular IP) subscribers concurrently with the MPLS/VPN-based subscribers, with the following limitations and requirements:

- The SM must work in "push" mode.
- Non-VPN-based subscribers cannot have IP in VPN mappings.
- VLAN-based subscribers are NOT supported at the same time as MPLS/VPN-based subscribers.

In typical MPLS/VPN networks, traffic that does not belong to any VPN is labeled with a single MPLS label in the upstream direction, which is used for routing. The downstream direction of such flows typically contains no label, due to penultimate hop popping.

The SCE platform uses the one or more labels upstream and no label downstream definition to identify non-VPN flows. Classification and traffic processor load balancing on these flows is performed according to the IP header, rather than the label.

This process requires learning of the upstream labels in use for such flows, and is done using the flow detection mechanism described above (see Flow Detection, page 13-3).

Bypassing Unknown VPNs

In an MPLS network, there may be many VPNs crossing the SCE platform, only a small number of which require service control functionality. It is necessary for the SCE platform to recognize which VPNs are not managed.

- The SCE platform automatically bypasses any VPN that is not configured in the SM
- The VPNs are bypassed by the SCE platform without any service

Note that the label limit (see Limitations, page 13-10)of 57,344 different labels includes labels from the bypassed VPNs.

Each bypassed VPN entry, both upstream and downstream, is removed from the database after a set period of time (10 minutes). If the entry is still used in the traffic, it will be re-learnt. This allows the database to remain clean, even if the labels are reused by the routers for different VPNs.

show bypassed VPNs In the **show bypassed VPNs** command, the age is indicated with each label - the length of time since it was learned.

Additional MPLS Pattern Support

The MPLS/VPN solution was designed to provide DPI services in MPLS/VPN network. These networks use BGP protocol as the control plane for the VPNs and LDP protocol for routing. There are complex networks where the MPLS infrastructure is used not only for VPN and routing, but also for other features such as traffic engineering (TE) and better fail-over. These features are usually enabled per VRF in the PE.

The Service Control MPLS/VPN solution does not support VPNs that use other MPLS-related features. Features such as MPLS-TE or MPLS-FRR (Fast Reroute) are not supported. VPNs for which these features are enabled can be automatically bypassed in the system, but are not allowed to be configured in the SM as serviced VPNs. Configuration of these VPNs in the SM might cause misclassification due to label aliasing.

The following list describes the labels combinations that are supported by the SCE platform and how each combination is interpreted by the platform:

- One or more labels upstream, no labels downstream:

  Assumed to be non-VPN (see Non-VPN-Based Subscribers, page 13-6).

  The SCE platform treats the following IP flows as non-VPN flows, and ignores their labels.

- One label upstream, one label downstream:

  Assumed to be VPN traffic, in which the P router happens to be the last hop in the upstream.

  The label in the downstream is treated as a BGP label, like the regular case. If the BGP label is known from the SM, then the flow is assigned to the correct subscriber, otherwise, it is treated as a bypassed VPN.

- Two labels upstream, one label downstream:

  This is the typical configuration of the system. Of the two upstream labels, one is for BGP and one for LDP. The downstream label is for BGP only

- More than two labels upstream, or more than one label downstream:

  These combinations occur when other MPLS-related features are enabled for the VPN. Such VPNs are not supported and should not be configured in the SM. However, they can be bypassed in the SCE platform without any service and without harming the service for other VPNs.

VPN Identifier (RD or RT)

Either the Route Distinguisher (RD) attribute or the Route Target (RT) attribute can be used to identify the VPN. It is required to decide which attribute best reflects the VPN partitioning, and configure the system accordingly. Note that the configuration is global for all the VPNs, that is, all VPNs must be identified by the same attribute.

The Route Distinguisher (RD) is generally used to distinguish the distinct VPN routes of separate customers who connect to the provider, so 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 VPNs that transfer information to a common central entity (for example 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 route, 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, consider using the RT as the VPN identifier.

It is important to note that this configuration is global. Therefore, if at some point in time, any VPN would have to be defined by RD, then all the other VPNs must be defined by RD as well. This is a point to consider when designing the initial deployment.

Service Control MPLS/VPN Requirements

Topology

Following are the general topology requirements for MPLS/VPN support:

- The SCE platform is placed in the network between the P routers (Provider MPLS core) and the PE (Provider Edge) routers.
- The subscriber side of the SCE platform is connected toward the PE router.
- The network side of the SCE platform is connected toward the P router.
- The BGP LEG is installed on the SM, and is placed somewhere in the network.

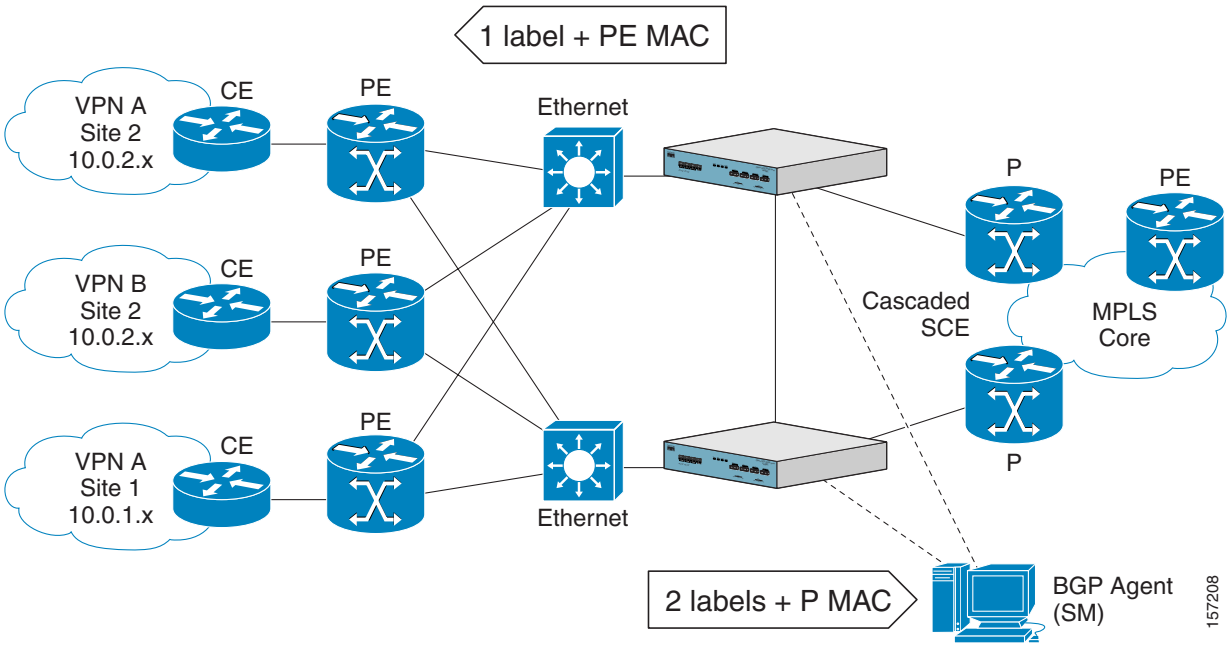
  It speaks with the SCE platform through the management IP.

In a cascade installation:

- The two SCE platforms are connected to each other via the cascade interfaces.
- The data link between the P and the PE is connected via the other interfaces on each SCE platform, as described above:
  - Subscriber side of each SCE platform connected toward the PE router
  - Network side of each SCE platform connected toward the P router

Figure 13-1 depicts a typical cascade installation.

Figure 13-1 Typical MPLs/VPN Installation



Capacity

The system supports:

- 2015 MPLS/VPNs
  - 80,000 IP mappings over VPNs
- 57,344 different labels (including upstream and downstream, and including the bypassed VPNs)
- 256 PEs per SCE platform
  - 4 interfaces per PE

Limitations

Mutually exclusive system modes

When the system works in MPLS/VPN mode, the following modes are not supported:

- The following tunneling modes:
  - MPLS traffic engineering skip
  - MPLS VPN skip
  - L2TP skip
  - VLAN symmetric classify
- TCP Bypass-establishment
- DDoS
- Value Added Services (VAS) mode

Number of MPLS labels

- The choice of the unique VPN site must be based on the BGP label only. The BGP label must be the innermost label.
- The MPLS/VPN solution supports various combinations of labels. See Additional MPLS Pattern Support.
- The system does not support VPNs for which other MPLS-related features, such as MPLS-TE or MPLS-FRR, are enabled.

Subscriber-related limitations

The following subscriber-related limitations exist in the current solution:

- The SM must be configured to operate in Push mode.
- VLAN-based subscribers cannot be used.
- Introduced subscriber aging is not supported when using VPN-based subscribers.
- Maximum number of VPN-based mappings per single subscriber:
  - 200 (standalone)
  - 50 (cascade)

Topology-related limitations

- An asymmetrical routing topology in which the traffic may be unidirectional, is not supported, since the MPLS/VPN solution relies on the bidirectional nature of the traffic for various mechanisms.

TCP related requirements

- Number of Upstream TCP Flows – There must be enough TCP flows opening from the subscriber side on each PE-PE route in each period of time. The higher the rate of TCP flows from the subscriber side, the higher the accuracy of the mechanism can be.

VPN configuration requirements

- Two VPN sites must be aggregated into one VPN if the following conditions are both true:
  - They are both connected to the same SCE platform
  - They both communicate with a common remote site using the same upstream labels and P router.
- An MPLS/VPN-based subscriber MAY NOT have IP mappings over more than one VPN.

Backwards Compatibility

An SCE platform running SCOS V3.1.5 and up does not support MPLS/VPN subscribers of the type used in older versions. Instead of defining an MPLS/VPN subscriber, which reflects the whole VPN, the user must configure a VPN entity and a full range private IP subscriber within that VPN (0.0.0.0/0@VPN1)

When working with the combination of SM of a version before V3.1.5LA and an SCE with V3.1.5 and up, only regular IP subscribers are supported. VPN-based subscribers are not supported at all in this combination.

Configuring MPLS/VPN Support

Configuring the MPLS Environment

In order for MPLS/VPN support to function, the environment must be configured correctly, specifically the following are required:

- All other tunneling protocols should be configured to the default mode.
- The MPLS auto-learning mechanism must be enabled.

How to Check the Running Configuration

Check the running configuration to verify no user-configured values appear for tunneling protocols or VLAN support, indicating that they are all in default mode.

Step 1 From the SCE# prompt, type `show running-config` and press **Enter**.

Displays the running configuration.

Step 2 Check that no VLAN or L2TP configuration appears.

How to Configure the MPLS Environment

If either VLAN or tunneling support is in default mode, skip the relevant step in the following procedure.

Step 1 From the SCE(config if)# prompt, type `default vlan` and press **Enter**.

Configures VLAN support to default mode.

Step 2 From the SCE(config if)# prompt, type `no IP-tunnel` and press **Enter**.

Disables all other tunneling protocol support.

Note All subscribers with VPN mappings must be cleared to change the tunneling mode. If the connection with the SM is down, use the **no subscriber all with-vpn-mappings** CLI command.

Note In addition, all VPN mappings must also be removed. This can only be done via the SM CLU (which means that the connection with the SM must be up).

Step 3 From the SCE(config if)# prompt, type `MPLS VPN auto-learn` and press **Enter**.

Enables the MPLS auto-learning mechanism.

Configuring the SCE Platform for MPLS/VPN Support

There are three main steps to configure the SCE platform for MPLS/VPN support:

1. Correctly configure the MPLS tunneling environment, disabling all other tunneling protocols, including VLAN support. (see How to Configure the MPLS Environment, page 13-12)
2. Define all PE routers, specifying the relevant interface IP addresses necessary for MAC resolution (see Defining the PE Routers, page 13-12.)
3. Configure the MAC resolver (see Configuring the MAC Resolver, page 13-14.)

Defining the PE Routers

Options

The following options are available:

- **PE-ID** — IP address that identifies the PE router.
- **interface-ip** — Interface IP address for the PE router. This is used for MAC resolution.
  - At least one interface IP address must be defined per PE router.
  - Multiple interface IP addresses may be defined for one PE router.
  - In the case where the PE router has multiple IP interfaces sharing the same MAC address, it is sufficient to configure just one of the PE interfaces
- **vlan** — A VLAN tag can optionally be provided for each interface IP.

Two interfaces cannot be defined with the same IP address, even if they have different VLAN tags. If such a configuration is attempted, it will simply update the VLAN tag information for the existing PE interface.

How to Add a PE Router

Each PE router that has managed VPNs behind it must be defined using the following CLI command.

Step 1 From the SCE(config if)# prompt, type **MPLS VPN PE-ID** *pe-id* **interface-ip-address** *interface-ip* **[vlan** *vlan***]** and press **Enter**.

Defines the PE router with with one interface IP address and optional VLAN tag. May also be used to add an additional interface IP address to an existing PE router.

How to Remove PE Routers

- About Removing PE Routers, page 13-13
- How to Remove a Specified PE Router, page 13-13
- How to Remove All PE Routers, page 13-14
- How to Remove a Specified Interface from a PE Router, page 13-14

About Removing PE Routers

Use these commands to remove one or all defined PE routers.

Please note the following:

- You cannot remove a PE if it retains any MPLS mappings. You must logout the VPN and remove all mappings before removing the router it uses. (You must use the SM CLU to remove VPN mappings.)
- Removing the last interface of a PE router removes the router as well. Therefore, you must logout the relevant VPN to remove the last interface.
- Likewise, all VPNs must be logged out before using the no PE-Database command below, since it removes all PE routers.

How to Remove a Specified PE Router

Step 1 From the SCE(config if)# prompt, type **no MPLS VPN PE-ID** *pe-id* and press **Enter**.

Removes the specified PE router.

How to Remove All PE Routers

Step 1 From the SCE(config if)# prompt, type **no MPLS VPN PE-Database** and press **Enter**.

Removes all configured PE routers.

How to Remove a Specified Interface from a PE Router

Step 1 From the SCE(config if)# prompt, type **no MPLS VPN PE-ID** *pe-id* **interface-ip-address** *interface-ip* and press **Enter**.

Removes the specified interface from the PE router definition. The PE router itself is not removed.

Configuring the MAC Resolver

About the MAC Resolver

The MAC resolver allows the SCOS to find the MAC address associated with a specific IP address. The MAC resolver must be configured when the SCE platform operates in MPLS/VPN mode, to translate the IP addresses of the provider edge router interfaces to their respective MAC addresses.

The MPLS/VPN mode needs the MAC resolver, as opposed to the standard ARP protocol, because ARP is used by the management interface, while MPLS/VPN uses the traffic interfaces of the SCE platform, which ARP does not include.

The MAC resolver database holds the IP addresses registered by the clients to be resolved. The IP addresses of the routers are added to and removed from the database in either of two modes:

- Dynamic mode (default)

  In this mode, the system listens to ARP messages of the configured PE interfaces, and this way it stays updated with their MAC addresses. There is no configuration required when operating in dynamic mode.

  - Benefit: it works even if the MAC address of the PE interface changes.
- Drawback: depending on the specific network topology, the MAC resolution convergence time may be undesirably long.

- Static mode

  In this mode, the MAC address of each PE router must be explicitly defined by the user.

  – Benefit: no initial delay until IP addresses converge

  – Drawback: PE interface is not automatically updated via ARP updates; therefore it doesn't automatically support cases where the MAC address changes on the fly.

  However, for statically configured MAC addresses, a user log message appears when the system detects that the MAC address changed. This can be used by the operator to configure the new address.

These two modes can function simultaneously; therefore selected PE routers can be configured statically, while the rest are resolved dynamically

Options

The following options are available:

- **ip address** — The IP address entry to be added to or removed from the database.
- **vlan tag** — VLAN tag that identifies the VLAN that carries this IP address (if applicable).
- **mac address** — MAC address assigned to the IP address, in xxxx.xxxx.xxxx format.

How to Add a Static IP Address

Step 1 From the SCE(config if)# prompt, type **mac-resolver arp** *ip_address* **[vlan** *vlan_tag***]** *mac_address* and press **Enter**.

Adds the specified IP address and MAC address pair to the MAC resolver database.

How to Remove a Static IP Address

Step 1 From the SCE(config if)# prompt, type **no mac-resolver arp** *ip_address* **[vlan** *vlan_tag***]** and press **Enter**.

Removes the specified IP address and MAC address pair from the MAC resolver database.

Monitoring the MAC Resolver

Use this command to see a listing of all IP addresses and corresponding MAC addresses currently registered in the MAC resolver database.

Step 1 From the SCE# prompt, type **show interface linecard 0 mac-resolver arp** and press **Enter**.

Displays a listing of all IP addresses and corresponding MAC addresses currently registered in the MAC resolver database.

Configuring the SM for MPLS/VPN Support

how to Configure the SM for MPLS/VPN Support

There are two main steps to configure the SM for MPLS/VPN support:

Step 1 Edit the *p3sm.cfg* configuration file to specify the field in the BGP messages that should be used by the SM for MPLS-VPN identification.

See How to Edit the SM Configuration File, page 13-16

Step 2 Install and configure the BGP LEG

Refer to the *Cisco SCMS SM LEGs User Guide* for more information.

How to Edit the SM Configuration File

The SM configuration file, *p3sm.cfg,* must be configured for the following:

- To specify the field in the BGP messages that should be used by the SM for MPLS-VPN identification.
- To enable IP ranges
- How to Configure the SM for MPLS/VPN Support, page 13-16
- How to Configure the SM for Troubleshooting MPLS/VPN Support, page 13-17

How to Configure the SM for MPLS/VPN Support

Step 1 Add the following section to the *p3sm.cfg* configuration file:

```
# The following section enables SM operation with MPLS-VPN support.
[MPLS-VPN]
# The following parameter defines the BGP attribute to use to identify VPN subscribers
# possible values: "rd" or "rt".
# (default: rt)
vpn_id=rt
```

How to Configure the SM for Troubleshooting MPLS/VPN Support

An optional parameter may be turned on to facilitate troubleshooting the BGP LEG installation. This parameter turns on detailed logging of messages received from the BGP LEG. It should only be turned on when necessary for troubleshooting and should always be turned off for normal operation of the system.

Step 1 Add the following parameter to the [MPLS-VPN] section of the *p3sm.cfg* configuration file:

```
# The following parameter turns on detailed logging of messages received from the BGP LEG
# should be changed to true only during troubleshooting
# (default: false)
log_all=true
```

How to Configure the SM to Allow IP Ranges

To setup the SM to work with MPLS/VPN, you must enable IP ranges by setting the **support_ip_ranges** in the configuration file.

Step 1 Set the **support_ip_ranges** parameter in the [Data Repository] section of the *p3sm.cfg* configuration file to 'yes', as in the following example.

```
support_ip_ranges=yes
```

Note Resetting this parameter requires restarting the SM. This parameter is discarded on regular configuration loading (using CLU).

Managing MPLS/VPN Support

Managing MPLS/VPN Support via SNMP

SNMP support for MPLS/VPN auto-learn is provided in two ways:

- MIB variables
- SNMP traps

MPLS/VPN MIB Objects

The mplsVpnAutoLearnGrp MIB object group (pcubeSEObjs 17) contains information regarding MPLS/VPN auto-learning.

The objects in the mplsVpnAutoLearnGrp provide the following information:

- maximum number of mappings
- allowed current number of mappings

For more information, see Appendix B, "Proprietary MIB Reference"

MPLS/VPN Traps

There is one MPLS/VPN-related trap:

- *mplsVpnTotalHWMappingsThresholdExceeded* (pcubeSeEvents 45)

To provide online notification of a resource deficiency, when the system reaches a level of 80% utilization of the hardware MPLS/VPN mappings, a warning message appears in the user log, and this SNMP trap is sent.

Both the warning and the trap are sent for each 100 mappings that are added after the threshold has been exceeded.

Monitoring MPLS/VPN Support via SCE Platform CLI

The SCE platform CLI allows you to do the following:

- Display VPN-related mappings
- Monitor subscriber counters
- Monitor PE routers
- Monitor bypassed VPNs

Displaying VPN-related Mappings

Use the following Viewer commands to display subscriber mappings. These commands display the following information:

- All the mappings for a specified VPN
- A listing of all currently logged-in VPNs
- A listing of all subscribers mapped to an IP range on a specified VPN
- The number of subscribers mapped to an IP range on a specified VPN
- The subscriber to whom a specified downstream mapping (PE loopback IP address and BGP label) is mapped. (This option is provided for backwards compatibility and has certain restrictions. See below How to Display the Name of the Subscriber Mapped to a Specified VPN, page 13-21.)

How to Display Mappings for a Specified VPN

Options

The following option is available:

- **vpn-name** — The name of the VPN for which to display mappings.

Step 1 From the SCE> prompt, type **show interface linecard 0 VPN name** *vpn-name* and press **Enter**.

Displaying Mappings for a Specified VPN: Examples

The following example illustrates the output of this command for an MPLS-based VPN.

```
SCE> show interface linecard 0 VPN name vpn1
VPN name: Vpn1
Downstream MPLS Mappings:
PE-ID = 1.0.0.1 Mpls Label = 20
PE-ID = 1.0.0.1 Mpls Label = 30
=======>Total Downstream Mappings: 2
Upstream MPLS Mappings:
=======>Total Upstream Mappings: 0
Number of subscriber mappings: 0
Explicitly introduced VPN
```

The following example illustrates the output of this command for a VLAN-based VPN

```
SCE> show interface linecard 0 VPN name vpn3
VPN name: Vpn3
VLAN: 2
Number of subscriber mappings: 0
Explicitly introduced VPN
```

The following example illustrates the output of this command for an automatically created VLAN VPN

```
SCE> show interface linecard 0 VPN name 2
VPN name: 2
VLAN: 2
Number of subscriber mappings: 1
Automatically created VPN
```

How to Display a Listing of all VPNs

Use this command to display a listing of all currently logged-in VPNs

Step 1 From the SCE> prompt, type **show interface linecard 0 VPN all-names** and press **Enter**.

Displaying a Listing of All VPNs: Example

```
SCE> show interface linecard 0 VPN all-names
```

How to Display Subscriber Mappings for an IP range on a Specified VPN

- Options, page 13-20
- Displaying Subscribers Mapped to a IP range on a Specified VPN: Example, page 13-20

Options

The following options are available:

- **ip-range** — The IP range for which to display mapped subscribers
- **vpn-name** — The name of the VPN for which to display mappings.

Step 1 From the SCE> prompt, type **show interface linecard 0 subscriber mapping included-in IP** *ip-range* **VPN** *vpn-name* and press **Enter**.

The VPN option allows you to search for subscribers with a private IP mapping

Displaying Subscribers Mapped to a IP range on a Specified VPN: Example

```
SCE> show interface linecard 0 subscriber mapping included-in IP 10.0.0.0/0 VPN vpn1
Subscribers with IP mappings included in IP range '10.0.0.0/0'@vpn1:
Subscriber 'Sub10', mapping '10.1.4.150/32@vpn1'.
Subscriber 'Sub10', mapping '10.1.4.149/32@vpn1'.
Subscriber 'Sub10', mapping '10.1.4.145/32@vpn1'.
Subscriber 'Sub11', mapping '10.1.4.146/32@vpn1'.
Total 2 subscribers found, with 4 matching mappings
```

How to Display the Number of Subscribers Mapped to an IP range on a Specified VPN

- Options, page 13-20
- Displaying the Number of Subscribers Mapped to range on a Specified VPN: Example, page 13-20

Options

The following options are available:

- **ip-range** — The IP range for which to display mapped subscribers
- **vpn-name** — The name of the VPN for which to display mappings.

Use the ‘**amount** ‘keyword to display the number of subscribers rather than a listing of subscriber names.

Step 1 From the SCE> prompt, type **show interface linecard 0 subscriber amount mapping included-in IP** *ip-range* **VPN** *vpn-name* and press **Enter**.

Displaying the Number of Subscribers Mapped to range on a Specified VPN: Example

```
SCE> show interface linecard 0 subscriber amount mapping included-in IP 0.0.0.0/0 VPN vpn1
There are 2 subscribers with 4 IP mappings included in IP range '0.0.0.0/0'.
```

How to Display the Name of the Subscriber Mapped to a Specified VPN

If the MPLS/VPN is configured as a single subscriber mapped to 0.0.0.0/0 on the VPN that is mapped to the specified MPLS, this option displays that subscriber

Note This command provides backward compatibility for MPLS/VPN subscriber configuration in SCOS versions previous to 3.1.5.

Step 1 From the SCE> prompt, type **show interface linecard 0 subscriber mapping MPLS-VPN PE-ID** *pe-id* **BGP-label** *label* and press **Enter**.

- Displaying the Subscriber Mapped to a Specified VPN: Example 1, page 13-21
- Displaying the Subscriber Mapped to a Specified VPN: Example 2, page 13-21

Displaying the Subscriber Mapped to a Specified VPN: Example 1

```
SCE>show interface lineCard 0 subscriber mapping MPLS-VPN PE-ID 1.0.0.1 BGP-label 30
BGP MPLS label 30 on PE 1.0.0.1 is mapped to VPN named 'Vpn1'
The VPN is NOT mapped to a single subscriber (0.0.0.0/0@Vpn1)
```

Displaying the Subscriber Mapped to a Specified VPN: Example 2

```
SCE>show interface lineCard 0 subscriber mapping MPLS-VPN PE-ID 1.0.0.1 BGP-label 30
BGP MPLS label 30 on PE 1.0.0.1 is mapped to VPN named 'Vpn1'
Subscriber 'Sub10' is mapped to 0.0.0.0/0@Vpn1
```

How to Display the Mappings of Upstream Labels that Belong to Non-VPN Flows

Step 1 From the SCE> prompt, type **show interface linecard 0 MPLS-VPN non-VPN-mappings** and press **Enter**.

Clearing Upstream VPN Mappings

Use this command to remove all learned upstream labels of a specified VPN.

Options

The following option is available:

- **vpn-name** — The name of the VPN for which to display mappings.

Step 1 From the SCE# prompt, type **clear interface linecard 0 VPN name** *vpn-name* **upstream mpls all** and press **Enter**.

This command, in effect, causes early label aging. Clearing the mappings allows relearning; labels will probably be quickly relearned after they have been cleared. Therefore, this command is useful when you want to update the VPN mappings without waiting for the standard aging period.

Monitoring Subscriber Counters

Use the following Viewer command to display subscriber counters, including those related to MPLS/VPN mappings.

About Subscriber Counters

When MPLS/VPN-based subscribers are enabled, the following related counters appear in addition to the basic subscriber counters:

- MPLS/VPN-based subscribers:
  - Current number of MPLS/-based subscribers that have VPN mappings.
  - Maximum number of MPLS/VPN-based subscribers
- MPLS/VPN-based subscribers are also counted in the general subscribers counters, but the general subscribers maximum number does not apply to MPLS/VPN-based subscribers, which have a smaller maximum number.
- MPLS/VPN mappings:
  - Current number of used MPLS/VPN mappings
  - Maximum number of MPLS/VPN mappings
- Note that these values reflect the total number of mappings, not just the mappings used by MPLS/VPN-based subscribers. Bypassed VPNs also consume MPLS/VPN mappings.

Step 1 From the SCE> prompt, type **show interface linecard 0 subscriber db counters** and press **Enter**.

Monitoring Subscriber Counters: Example

```
SCE>show interface linecard 0 subscriber db counters
Current values:
===============
Subscribers: 2 used out of 99999 max.
Introduced subscribers: 2.
Anonymous subscribers: 0.
Subscribers with mappings: 2 used out of 99999 max.
SINGLE non-VPN IP mappings: 1.
non-VPN IP Range mappings: 1.
IP Range over VPN mappings: 1.
Single IP over VPN mappings: 3.
MPLS-based subscribers are enabled.
MPLS/VPN mappings: 2 used out of 57344 max.
MPLS based VPNs with subscriber mappings: 2 used out of 2015 max.
Subscribers with open sessions: 0.
Subscribers with TIR mappings: 0.
Sessions mapped to the default subscriber: 0.
Peak values:
============
Peak number of subscribers with mappings: 2
Peak number occurred at: 14:56:55 ISR MON June 9 2007
Peak number cleared at: 15:29:39 ISR MON June 9 2007
Event counters:
===============
Subscriber introduced: 2.
```

```
Subscriber pulled: 0.
Subscriber aged: 0.
Pull-request notifications sent: 0.
State notifications sent: 0.
Logout notifications sent: 0.
Subscriber mapping TIR contradictions: 0
```

Monitoring MPLS/VPN Counters

Use the following Viewer command to display MPLS/VPN information.

Step 1 From the SCE> prompt, type **show interface linecard 0 mpls vpn** and press **Enter**.

Monitoring MPLS/VPN Counters: Example

```
SCE> show interface linecard 0 mpls vpn
MPLS/VPN auto-learn mode is enabled.
MPLS based VPNs with subscriber mappings: 0 used out of 2015 max
Total HW MPLS/VPN mappings utilization: 0 used out of 57344 max
MPLS/VPN mappings are divided as follows:
downstream VPN subscriber mappings: 0
upstream VPN subscriber mappings: 0
non-vpn upstream mappings: 0
downstream bypassed VPN mappings: 0
upstream bypassed VPN mappings: 0
```

Monitoring the PE Routers

Use the following Viewer commands to monitor PE routers. These commands provide the following information:

- Configuration of all currently defined PE routers.
- Configuration of a specified PE router.
- How to Display the Configuration of all Currently Defined PE Routers, page 13-23
- How to Display the Configuration of a Specified PE Router, page 13-23

How to Display the Configuration of all Currently Defined PE Routers

Step 1 From the SCE> prompt, type **show interface linecard 0 MPLS VPN PE-Database** and press **Enter**.

How to Display the Configuration of a Specified PE Router

Step 1 From the SCE# prompt, type **show interface linecard 0 MPLS VPN PE-Database PE-ID** *pe-id* and press **Enter**.

Monitoring Bypassed VPNs

How to Display the Currently Bypassed VPNs

Step 1 From the SCE> prompt, type **show interface linecard 0 MPLS VPN Bypassed-VPNs** and press **Enter**.

How to Remove all Learned Bypassed VPNs

Step 1 From the SCE# prompt, type **clear interface linecard 0 MPLS VPN Bypassed-VPNs** and press **Enter**.

Monitoring Non-VPN Mappings

How to Display Non-VPN Mappings

Step 1 From the SCE> prompt, type **show interface linecard 0 MPLS VPN non-VPN-mappings** and press **Enter**.

How to Remove all Learned non-VPN Mappings

Step 1 From the SCE# prompt, type **clear interface linecard 0 MPLS VPN non-VPN-mappings** and press **Enter**.

Managing MPLS/VPN Support via SM CLU

The SM CLU allows you to do the following:

- Add and remove VPNs
- Display VPN information
- Clear MPLS/VPN mappings

For more information, see the *Cisco Service Control Management Suite Subscriber Manager User Guide*.

Managing VPNs

Use the **p3vpn** utility to manage VPNs.

Options

The following options are available:

- **VPN-Name** — The name assigned to the VPN when it was added, or, if adding a VPN, the name to be assigned to it.
- **RT@PE-IP** — The mapping assigned to the VPN. Multiple mappings can be specified using a comma.
  - **RT** = the route target of the VPN, specified using the ASN:n notation or the IP:n notation

  Note that the Route Distinguisher may be specified rather than the route target
  - PE-IP = the loopback IP of the PE router connected to that VPN

How to Add a New MPLS-based VPN

Step 1 From the shell prompt, type the following command: `p3vpn --add --vpn=`*`VPN-Name`* `--mpls-vpn=`*`RT@PE,(RT@PE2, RT@PE3,....`*

How to Remove a VPN

Step 1 From the shell prompt, type the following command: `p3vpn --remove --vpn=`*`VPN-Name`*

How to Display VPN Information

To List All Existing VPNs

Step 1 From the shell prompt, type the following command: `p3vpn --show-all`

To List All Subscribers for a Specified VPN

Step 1 From the shell prompt, type the following command: `p3vpn --show-sub --vpn=`*`VPN-Name`*

Listing All Subscribers for a Specified VPN: Example

```
p3vpn –show-sub --vpn=vpn1
sub1: 10.1.1.0/24@vpn1
sub2: 20.1.1.0/24@vpn1
Command terminated successfully
```

To Display the Mappings for a Specified VPN

Step 1 From the shell prompt, type the following command: `p3vpn --show --vpn=`*`VPN-Name`*

Listing All Subscribers for a Specified VPN: Example

```
p3vpn --show --vpn=vpn1
Name:           vpn1
Domain:         subscribers
Mappings:
MPLS/VPN: 1:1000@10.0.0.1       (no BGP information)
MPLS/VPN: 1:1000@10.0.0.2       label: 10 IP range: 1.1.1.1/32
Command terminated successfully
```

How to Manage VPN Mappings

- To Remove All Existing Mappings from a Specified VPN, page 13-26
- To Remove a Specified Mapping from a Specified VPN, page 13-26

To Remove All Existing Mappings from a Specified VPN

Step 1 From the shell prompt, type the following command: **p3vpn –-remove-all-mappings --vpn=VPN-Name**

To Remove a Specified Mapping from a Specified VPN

Step 1 From the shell prompt, type the following command: **p3vpn –-remove-mappings --vpn=VPN-Name --mpls-vpn=RT@PE,(RT@PE2, RT@PE3,...)**

How to Add Mappings to VPN-based Subscribers

There are three types of mappings that can be added to an existing VPN-based subscriber:

- A set of IP addresses defined as IP@VPN
- A complete VPN (this is actually a special case of IP@VPN mappings, in which the mapping is defined as 0.0.0.0/0@VPN)
- All the IP addresses of a CE router, defined by a AS:value@VPN-NAME (BGP community)

How to Add IP Address Mappings

Options

The following options are available

- **SUB-NAME** — The name of the subscriber to be associated with the specified community attribute
- **IP1[/RANGE][,...]@VPN-NAME** — IP address or addresses to assign to the VPN
  - **IP** = the IP address. This may be any of the following
  - a single IP address (x.x.x.x)
  - a single range of IP addresses (x.x.x.x/y)
  - a list of IP addresses separated by commas (x.x.x.x, y.y.y.y, z.z.z.z)
  - a list of IP address ranges (x.x.x.x/a, y.y.y.y/b, z.z.z.z/c)
  - **VPN-NAME** = name of the VPN to which the community attribute will be assigned
- **--additive-mappings** — Use this option to add the new mapping(s) to any existing ones. (Without this option, any existing mappings are overwritten.)

Step 1 From the shell prompt, type the following command: **p3subs –-add -–subscriber=SUB-NAME --ip=IP1[/RANGE][,...]@VPN-NAME [--additive-mappings]**

How to Add VPN-based Mappings

This option is supported to provide backwards compatibility with MPLS/VPN-based subscribers in releases before 3.1.5.

Options

The following options are available

- **SUB-NAME** — The name of the subscriber to be associated with the specified community attribute
- **VPN-NAME** — The name of the VPN to which the subscriber will be mapped. (This option is equivalent to defining the mapping as 0.0.0.0/0@VPN)
- **--additive-mappings** — Use this option to add the new mapping(s) to any existing ones. (Without this option, any existing mappings are overwritten.)

Step 1 From the shell prompt, type the following command: **p3subs –-add -–subscriber=SUB-NAME –-vpn=VPN-NAME [--additive-mappings]**

How to Configure the Community Parameter

An optional parameter may be set defining a community attribute. The community attribute provides a mechanism for defining the BGP community as one subscriber, using the *community@VPN* specification.

The community attribute in the BGP protocol is used to dynamically map IP ranges to subscribers. The community attribute can be configured in the Provider Edge (PE) router or in the Customer Edge (CE) router.

The *community@VPN* specification is replaced by an IP@VPN specification by the BGP LEG.

Use the **p3subs** utility to configure the community parameter.

Options

The following options are available:

- **SUB-NAME** — The name of the subscriber to be associated with the specified community attribute
- **AS:value@VPN-NAME** — The community attribute to assign to the VPN
  - **AS** = autonomous system. Integer in the range 0-65535 assigned by the network administrator
  - **value** = the community attribute. Integer in the range 0-65535 assigned by the network administrator
  - **VPN-NAME** = name of the VPN to which the community attribute will be assigned

Step 1 From the shell prompt, type the following command: **p3subs –-add –-subscriber=SUB-NAME --community=AS:value@VPN-NAME**

How to Remove VPN Mappings from Subscribers

To Remove All Existing Mappings from a Specified Subscriber

Step 1 From the shell prompt, type the following command: **p3subs –-remove-all-mappings –-subscriber=SUB-NAME**

To Remove a Specified IP Mapping from a Specified Subscriber

Step 1 From the shell prompt, type the following command: **p3psubs –-remove-mappings –-subscriber=SUB-NAME --ip=IP1[/RANGE][,...]@VPN-NAME**

To Remove a Specified VPN Mapping from a Specified Subscriber

Step 1 From the shell prompt, type the following command: **p3psubs –-remove-mappings --–subscriber=SUB-NAME --vpn=VPN-NAME**

To Remove a Specified Community-based Mapping from a Specified Subscriber

Step 1 From the shell prompt, type the following command: **p3psubs –-remove-mappings --–subscriber=SUB-NAME --community=AS:value@VPN-NAME**

How to Monitor Subscriber MPLS/VPN Mappings

Use the **p3subs** utility to manage VPNs.

Step 1 From the shell prompt, type the following command: **p3subs --show-all-mappings --subscriber=SUB-NAME**