



CISCO SERVICE CONTROL SOLUTION GUIDE



Cisco Service Control MPLS/VPN Solution Guide, Release 3.7.x

- 1** About this Guide
- 2** Introduction to the Service Control MPLS/VPN Solution
- 3** Overview of the Service Control Solution for MPLS/VPN Networks
- 4** Configuring MPLS/VPN Support
- 5** Managing MPLS/VPN Support
- 6** Obtaining Documentation and Submitting a Service Request



Note This document supports all 3.7.x releases.

1 About this Guide

Cisco Service Control MPLS/VPN Solution Guide is for experienced network administrators who are responsible for configuring and maintaining the Service Control Multiprotocol Label Switching (MPLS) or VPN solution.

Document Revision History

Table 1 lists the Document Revision History, which records the changes to this document.

Table 1 Document Revision History

Revision	Cisco Service Control Release and Date	Change Summary
OL-24165-01	Supports all 3.7.x releases June 13, 2011	First version of this document.

Related Publications

For additional information about the components of the Cisco Service Control MPLS/VPN solution, see the related documentation:

- For more information about general configuration of the Cisco Service Control solution, see these guides:
 - *Cisco SCE 8000 10GBE Software Configuration Guide*
 - *Cisco SCE 8000 GBE Software Configuration Guide*
 - *Cisco SCE 2000 and SCE 1000 Software Configuration Guide*
- For more information about the Service Control CLI and a complete listing of all CLI commands, see these command reference guides:
 - *Cisco SCE 8000 CLI Command Reference*
 - *Cisco SCE 2000 and SCE 1000 CLI Command Reference*
- For more information about the configuration and maintenance of the Subscriber Manager, see *Cisco Service Control Management Suite Subscriber Manager User Guide*.

In addition, the extensive features and functionality of the SCE platform and the softwares are documented in these guides:

- For complete installation information, including initial configuration, see these installation guides:
 - *Cisco SCE 8000 10GBE Installation and Configuration Guide*
 - *Cisco SCE 8000 GBE Installation and Configuration Guide*
 - *Cisco SCE 2000 Installation and Configuration Guide*
 - *Cisco SCE 1000 2xGBE Installation and Configuration Guide*



Note You can access Cisco software configuration, and hardware installation and maintenance documentation at the Cisco.com.

- For initial installation and startup information, see these quick start guides:
 - *Cisco SCE 8000 10GBE Quick Start Guide*
 - *Cisco SCE 8000 GBE Quick Start Guide*
 - *Cisco SCE 2000 Quick Start Guide*
 - *Cisco Service Control Engine 1000 2xGBE Quick Start Guide*
- For international agency compliance, safety, and statutory information for WAN interfaces for the SCE platform, see the regulatory and safety information document:
 - *Regulatory Compliance and Safety Information for the Cisco Service Control Engine (SCE)*

2 Introduction to the Service Control MPLS/VPN Solution

This section explains how the Cisco Service Control MPLS/VPN solution was developed to cope with the challenges faced by ISPs offering MPLS/VPN services.

Cisco Service Control MPLS/VPN: The Challenge and The Solution

- [Overview, page 4](#)
- [Challenge, page 4](#)
- [Cisco MPLS/VPN Service Control Solution, page 4](#)
- [Benefits for Service Providers, page 5](#)

Overview

Cisco offers a Service Control solution for service providers who are either offering MPLS/VPN services to their customers, or planning to introduce such a service in the near future. This solution targets providers offering enterprise-focused solutions as well as those involved in offering MPLS/VPN services to their small office, home office (SOHO) customers. This highest level solution allows complete visibility into the applications and services in MPLS/VPN tunnels for subscriber-based usage monitoring and billing, and is used for capacity control and differentiation of service levels as well.

The Service Control solution incorporates the ability to monitor and control all the traffic in an MPLS/VPN tunnel as belonging to a single subscriber entity, including traffic with private non-routable IP addresses. Its advanced functionality facilitates the implementation of the Cisco Service Control solution in MPLS/VPN environments, and the suite of capabilities that the solution provides.

Challenge

Service providers who offer MPLS/VPN services are challenged in their ability to use their investment in the MPLS/VPN infrastructure. This hampers their ability to both reduce total cost of ownership and increase per customer revenue, aggregate revenue, and profitability.

These service providers need to:

- Implement usage monitoring and trend analysis for the traffic of MPLS/VPN tunnels to improve existing business models and develop new ones.
- Launch new service packages and billing plans enabled by granular subscriber usage information per service and per application for the traffic inside MPLS/VPN tunnels.
- Control the traffic inside MPLS/VPN tunnels by de-prioritizing some of the traffic that the MPLS/VPN customers consider less important, while prioritizing business-critical traffic and providing network-based services, such as content-filtering, security phishing prevention, and other such services.

Cisco MPLS/VPN Service Control Solution

In the Cisco MPLS/VPN Service Control solution, Cisco has managed to overcome the technical challenge of classifying flows with private non-routable IP addresses into the correct MPLS/VPN that these flows are part of. The challenge originates from the fact that the SCE platform may have been incorrectly classifying the packets of these flows. The Cisco MPLS/VPN solution implements a unique learning algorithm that can successfully, reliably, and correctly classify multiple flows in multiple MPLS/VPN tunnels, even if they have the same private IP address.

The Cisco MPLS/VPN Service Control solution:

- Closes the loop between the Service Control engine and the provider edge (PE) routers that manage the allocation of MPLS tags to MPLS/VPN tunnels.
- Overcomes the challenge of correct classification of flows with private non-routable source-IP addresses.

Benefits for Service Providers

With the Cisco Service Control MPLS/VPN solution, service providers can benefit from granular per-subscriber and per-application usage reports. This granularity allows for complete per subscriber and per application Layer-7 visibility of the manner in which the MPLS/VPN subscribers use the service provider's network. The reports can, for example, show these details:

- HTTP hosts or Real Time Streaming Protocol (RTSP) streaming hosts that are most popular for each subscriber.
- Bandwidth per service consumed by an MPLS/VPN subscriber over a predefined time period.
- Extensive variety of usage reports available as part of the Cisco Service Control solution.

These reports can be used by the service provider network teams for capacity planning, and by the marketing teams for planning and rolling out new *tiers of service* packages.

In addition to the data records that enable these reports, the solution also generates data records that can be forwarded to mediation and billing systems and used for implementation of granular usage-based billing.

Service providers can also benefit from the Service Control MPLS/VPN solution by using the SCE platforms as network enforcement devices for a variety of per-network-based services, such as:

- Prioritizing mission-critical traffic —SCE platforms can be used for prioritizing the Oracle or Citrix traffic that flows between the branches of the MPLS/VPN customer.
- Implementing various types of managed services —The Cisco MPLS/VPN solution can be used to create services designed to increase employee productivity, such as the creation of a network-based content filtering service. The deployment, management, and ongoing administration of this suite of services can be easily controlled using a standard web interface.

This flexibility not only provides an extremely attractive return on investment, but protects your investment as your needs for network and application infrastructure evolve.

Using the Service Control infrastructure to create these next-generation services provides the path to enhanced customer revenue streams, differentiated service offerings, and a cost structure commensurate with the required business model.

3 Overview of the Service Control Solution for MPLS/VPN Networks

This section contains these subsections:

- [Service Control in the MPLS/VPN Environment, page 6](#)
- [Definitions and Acronyms, page 6](#)
- [Challenges for Service Control MPLS/VPN Support, page 7](#)
- [How MPLS/VPN Support Works, page 7](#)
- [Service Control MPLS/VPN Concepts, page 10](#)
- [Service Control MPLS/VPN Requirements, page 11](#)

Service Control in the MPLS/VPN Environment

MPLS/VPN networks are very complex, and use 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:

- MPLS/VPN architecture is in accordance with RFC 2547.
- 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—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 penultimate-hop popping (PHP) or other reasons.
 - Internal labels [Border Gateway Protocol (BGP) labels]—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 Subscriber Manager. The Subscriber Manager 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 the [“Non-VPN-Based Subscribers”](#) section on page 10.)

Definitions and Acronyms

Table 2 defines important terms and acronyms.

Table 2 *MPLS/VPN Terms and Acronyms*

Term or Acronym	Definition
PE ¹	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 ²	Router in the core of the service provider network. P routers forward only MPLS packets, regardless of VPNs.
VPN	In the Service Control context, a VPN resides in a specific site. It is a managed entity over which private IP subscribers can be managed.

Table 2 MPLS/VPN Terms and Acronyms (continued)

Term or Acronym	Definition
BGP LEG	Software module that resides on the Subscriber Manager server and generates BGP-related login events. The BGP LEG communicates with the BGP routers (PEs) and passes the relevant updates to the Subscriber Manager 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 ³	Used to uniquely identify the same network and mask from different VRFs (such as, 10.0.0.0/8 from VPN A and 10.0.0.0/8 from VPN B).
RT ⁴	Used by the routing protocols to control import and export policies, to build arbitrary VPN topologies for customers.
VRF ⁵	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.

1. PE = Provider Edge
2. P = Provider
3. RD = Route Distinguisher
4. RT = Route Target
5. VRF = Virtual Routing and Forwarding

Challenges for Service Control MPLS/VPN Support

The challenges involved in providing Service Control MPLS/VPN support are:

- 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 and the MAC address of the PE.

How MPLS/VPN Support Works

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

- Flow detection—SCE platforms match upstream and downstream traffic to identify flows.
- VPN detection—Downstream VPN labels are identified by the Subscriber Manager. The SCE platform learns the upstream labels from the traffic to identify the VPN.
- Subscriber detection—Subscriber Manager and 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 Cisco Service Control Operating System (Cisco SCOS) uses to identify flows, and notes that in MPLS, the packet is labeled differently in each direction.

Because MPLS traffic is unidirectional, each direction is classified separately by the SCE platform, using these:

- Downstream—BGP label and the MAC address of the PE router (only one label that is relevant to the classification)
Downstream labels are learned from the control plane (through the Subscriber Manager BGP Login Event Generator (LEG)).
- Upstream—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 Subscriber Manager. The network-wide value that describes a VPN most closely is either the RT or the RD.

- Administrator configures the Subscriber Manager to detect VPNs, according to selected attribute (RT or RD). (See the [“How to Configure the Subscriber Manager for MPLS/VPN Support”](#) section on page 17).
- Network operator provides the SCE platform with a mapping between RT values and VPN subscriber names. (See the [How to Manage MPLS/VPN Support via Subscriber Manager CLU](#), page 25).

The relevant module in the Subscriber Manager server 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 router 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 Subscriber Manager. The SCE platform CLI can be used to view VPN-related information, but not to configure the VPNs.

Subscriber Detection

This section consists of these subsections:

- [MPLS/VPN Based Subscriber](#), page 8
- [Private IP Subscriber Support](#), page 8

MPLS/VPN Based Subscriber

In MPLS/VPN (as in other modes of operation), 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 these:

- Set of IP addresses or ranges in a certain VPN
- All the IP addresses of a customer edge (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 Subscriber Manager. (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. Because 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, 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 are 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

This section consists of these subsections:

- [How the Service Control MPLS/VPN Solution Works: A Summary, page 9](#)
- [SCE Platform Tasks in the MPLS/VPN Solution, page 9](#)
- [BGP LEG Tasks in the MPLS/VPN Solution, page 9](#)
- [Subscriber Manager Tasks in the MPLS/VPN Solution, page 9](#)

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

- The Subscriber Manager is configured with the VPNs and VPN-based subscribers that should be managed. A VPN is identified by the RD or RT and the PE router.
- BGP LEG updates the Subscriber Manager with the MPLS labels and IP routes.
- The Subscriber Manager 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, and so forth).

SCE Platform Tasks in the MPLS/VPN Solution

- Matches upstream to downstream labels:
 - Mappings of downstream labels to VPNs are received from the Subscriber Manager
 - Upstream labels are learned from the data
- Uses MAC addresses of the PEs to distinguish downstream labels of different PEs.
- After the learning, classifies each flow as belonging to one of the VPNs.
- Performs a longest prefix match on the IP address inside the VPN, and classifies each flow to the correct VPN-based subscriber.
- Runs the Cisco SCA BB 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

BGP LEG is a software module that runs on the Subscriber Manager server.

- 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 Subscriber Manager module.

Subscriber Manager Tasks in the MPLS/VPN Solution

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

Service Control MPLS/VPN Concepts

- [Non-VPN-Based Subscribers, page 10](#)
- [Bypassing Unknown VPNs, page 10](#)
- [Additional MPLS Pattern Support, page 10](#)
- [VPN Identifier \(RD or RT\), page 11](#)

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 these limitations and requirements:

- Subscriber Manager 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 does not contain any label, because of PHP.

The SCE platform uses 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 the [“Flow Detection” section on page 7](#)).

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 Subscriber Manager.
- VPNs are bypassed by the SCE platform without any service.



Note The label limit (see the [“Limitations” section on page 12](#)) of 57344 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 is re-learned. This allows the database to remain clean, even if the labels are reused by the routers for different VPNs.

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

Additional MPLS Pattern Support

The MPLS/VPN solution was designed to provide deep packet inspection (DPI) services in an MPLS/VPN network. These networks use BGP as the control plane for the VPNs and Label Distribution Protocol (LDP) for routing. There are complex networks in which 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 Cisco 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 Subscriber Manager as serviced VPNs. Configuration of these VPNs in the Subscriber Manager might cause misclassification because of label aliasing.

This list describes the label 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 the [“Non-VPN-Based Subscribers” section on page 10](#)).
The SCE platform treats these 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.
Label in the downstream is treated as a BGP label, like the regular case. If the BGP label is known from the Subscriber Manager, then the flow is assigned to the correct subscriber, otherwise, it is treated as a bypassed VPN.
- Two labels upstream, one label downstream—Typical configuration of the system. Of the two upstream labels, one is for BGP and one for LDP. The downstream label is only for BGP.
- More than two labels upstream, or more than one label downstream—Combinations that occur when other MPLS-related features are enabled for the VPN. Such VPNs are not supported and should not be configured in the Subscriber Manager. 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 RD attribute or the 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. The configuration is global for all the VPNs, that is, all VPNs must be identified by the same attribute.

RD is generally used to distinguish the distinct VPN routes of separate customers who connect to the provider, so in most cases RD is a good partition for the VPNs in the network. Because 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, and so forth).

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 must be treated as a single subscriber, consider using 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, 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

This section consists of these subsections:

- [Topology, page 11](#)
- [Capacity, page 12](#)
- [Limitations, page 12](#)
- [Backwards Compatibility, page 13](#)

Topology

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

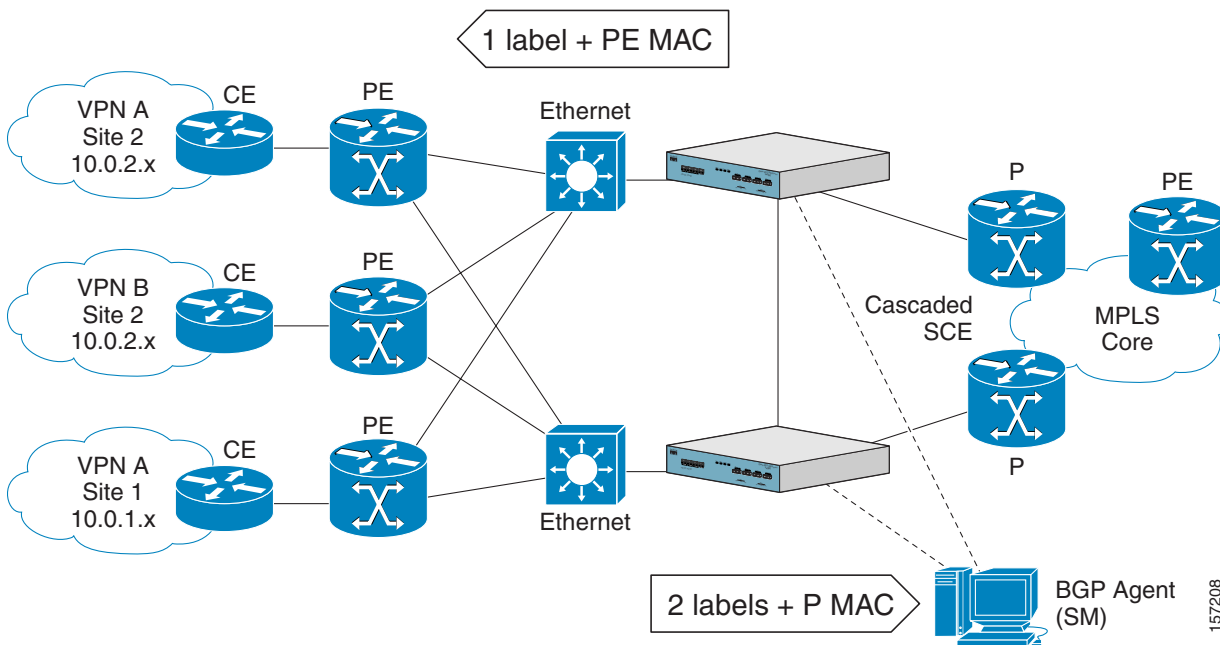
- SCE platform is placed in the network between the P routers (Provider MPLS core) and the PE routers.
- Subscriber side of the SCE platform is connected to the PE router.
- Network side of the SCE platform is connected to the P router.
- BGP LEG is installed on the Subscriber Manager, and is placed 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 1 depicts a typical cascade installation.

Figure 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



Note MPLS/VPN functionality is not supported on the Cisco SCE 8000 platform.

The limitations are:

- [Mutually Exclusive System Modes, page 13](#)
- [Number of MPLS Labels, page 13](#)
- [Subscriber-Related Limitations, page 13](#)
- [Topology-Related Limitations, page 13](#)
- [TCP-Related Requirements, page 13](#)
- [VPN Configuration Requirements, page 13](#)

Mutually Exclusive System Modes

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

- Tunneling modes:
 - Cisco MPLS TE skip
 - MPLS/VPN skip
 - Layer 2 Tunneling Protocol (L2TP) skip
 - VLAN symmetric classify
- TCP bypass establishment
- Distributed denial of service (DDoS)
- Value Added Services (VAS)

Number of MPLS Labels

- Choice of the unique VPN site must be based only on the BGP label. The BGP label must be the innermost label.
- MPLS/VPN solution supports various combinations of labels. See the [“Additional MPLS Pattern Support” section on page 10](#).
- Systems do not support VPNs for which other MPLS-related features, such as MPLS-TE or MPLS-FRR, are enabled.

Subscriber-Related Limitations

These subscriber-related limitations exist in the current solution:

- The Subscriber Manager 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

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

TCP-Related Requirements

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.

VPN Configuration Requirements

These are the VPN configuration requirements:

- Two VPN sites must be aggregated into one VPN if these conditions are both true:
 - Connected to the same SCE platform
 - Communicate with a common remote site by 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 later does not support MPLS/VPN subscribers of the type used in earlier 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 Subscriber Manager (version earlier than 3.1.5) and an SCE (Version 3.1.5 and later), only regular IP subscribers are supported. VPN-based subscribers are not supported.

4 Configuring MPLS/VPN Support

This section explains how to configure MPLS/VPN support. Both the SCE platform and the Subscriber Manager must be configured correctly.

- [Configuring the MPLS Environment, page 14](#)
- [Configuring the SCE Platform for MPLS/VPN Support, page 15](#)
- [How to Configure the Subscriber Manager for MPLS/VPN Support, page 17](#)

Configuring the MPLS Environment

For MPLS/VPN support to function, the environment must be configured correctly. It specifically requires that:

- All other tunneling protocols are configured to the default mode.
- MPLS auto-learning mechanism is enabled.

How to Check the Running Configuration

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

Step 1 At the SCE# prompt, enter **show running-config** and press **Enter**.

The running configuration appears.

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 these procedure:

Step 1 At the SCE(config if)# prompt, enter **default vlan** and press **Enter**.

This configures VLAN support to default mode.

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

This disables all other tunneling protocol support.



Note All subscribers with VPN mappings must be cleared to change the tunneling mode. To clear all subscribers with VPN mappings when the Subscriber Manager is down, use the **no subscriber all with-vpn-mappings** CLI command.



Note In addition, all VPN mappings must also be removed. This can be done only via the Subscriber Manager CLU (which means that the connection with the Subscriber Manager must be up). See the [“How to Manage VPN Mappings” section on page 26](#).

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

This enables the MPLS auto-learning mechanism.

Configuring the SCE Platform for MPLS/VPN Support

This section consists of these subsections:

- [About Configuring the SCE Platform for MPLS/VPN Support, page 15](#)
- [How to Define the PE Routers, page 15](#)
- [How to Configure the MAC Resolver, page 16](#)
- [How to Monitor the MAC Resolver, page 17](#)

About 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 by disabling all other tunneling protocols, including VLAN support. (See the “[How to Configure the MPLS Environment](#)” section on page 14.)
2. Define all PE routers, specifying the relevant interface IP addresses necessary for MAC resolution. (See the “[How to Define the PE Routers](#)” section on page 15.)
3. Configure the MAC resolver. (See the “[How to Configure the MAC Resolver](#)” section on page 16.)

How to Define the PE Routers

This sections consists of these subsections:

- [Options, page 15](#)
- [How to Add a PE Router, page 15](#)
- [How to Remove PE Routers, page 16](#)

Options

These options are available:

- **PE-ID**—IP address that identifies the PE router.
- **interface-ip**—Interface IP address for the PE router. 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**—(Optional) Can 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 simply updates 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 **MPLS VPN PE-ID pe-id interface-ip-address interface-ip [vlan vlan]** command at the **SCE(config if)#** prompt.

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

How to Remove PE Routers

This section consists of these subsections:

- [About Removing PE Routers, page 16](#)
- [How to Remove a Specified PE Router, page 16](#)
- [How to Remove All PE Routers, page 16](#)
- [How to Remove a Specified Interface from a PE Router, page 16](#)

About Removing PE Routers

Use the commands specified in this section to remove one or all defined PE routers.

Note the following:

- You cannot remove a PE, if it retains any MPLS mappings. The VPN must be logged out and all mappings removed before removing the router used. (You must use the Subscriber Manager command line utility (CLU) to remove VPN mappings. See the [“How to Manage VPN Mappings” section on page 26.](#))
- 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 because it removes all PE routers.

How to Remove a Specified PE Router

At the SCE(config if)# prompt, enter **no MPLS VPN PE-ID pe-id** and press **Enter**.

This command removes the specified PE router.

How to Remove All PE Routers

At the SCE(config if)# prompt, enter **no MPLS VPN PE-Database** and press **Enter**.

This command removes all configured PE routers.

How to Remove a Specified Interface from a PE Router

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

This command removes the specified interface from the PE router definition. The PE router itself is not removed.

How to Configure the MAC Resolver

This section consists of these subsections:

- [About the MAC Resolver, page 16](#)
- [Options, page 17](#)
- [How to Add a Static IP Address, page 17](#)
- [How to Remove a Static IP Address, page 17](#)

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 PE router interfaces to their respective MAC addresses.

The MPLS/VPN mode needs the MAC resolver, as opposed to the standard ARP protocol, because the ARP is used by the management interface, whereas 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)**—System listens to ARP messages of the configured PE interfaces, and this way it stays updated with their MAC addresses. No configuration is 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**—MAC address of each PE router must be explicitly defined by the user.
 - **Benefit**—There is no initial delay until the IP addresses converge.
 - **Drawback**—PE interface is not automatically updated via ARP updates; therefore, it does not 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.

For more information about the MAC resolver, see these configuration guides:

- *Cisco SCE 8000 10GBE Software Configuration Guide*
- *Cisco SCE 8000 GBE Software Configuration Guide*
- *Cisco SCE 2000 and SCE 1000 Software Configuration Guide*

Options

These options are available:

- **ip address**—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 enter the IP address, in *xxxx.xxxx.xxxx* format.

How to Add a Static IP Address

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

This command adds the specified IP address and MAC address pair to the MAC resolver database.

How to Remove a Static IP Address

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

This command removes the specified IP address and MAC address pair from the MAC resolver database.

How to Monitor the MAC Resolver

At the SCE# prompt, enter **show interface linecard 0 mac-resolver arp** and press **Enter**.

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

How to Configure the Subscriber Manager for MPLS/VPN Support

This section consists of these subsections:

- [Configuring the Subscriber Manager for MPLS/VPN Support, page 18](#)
- [How to Edit the Subscriber Manager Configuration File, page 18](#)
- [How to Configure the Subscriber Manager to Allow IP Ranges, page 18](#)

Configuring the Subscriber Manager for MPLS/VPN Support

There are two main steps to configure the Subscriber Manager 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 Subscriber Manager for MPLS/VPN identification. See the [“How to Edit the Subscriber Manager Configuration File” section on page 18](#).
- Step 2** Install and configure the BGP Login Event Generator (LEG).
For more information, see the *Cisco SCMS SM LEGs User Guide*.
-

How to Edit the Subscriber Manager Configuration File

The Subscriber Manager configuration file, `p3sm.cfg`, must be configured to:

- Specify the field in the BGP messages that should be used by the Subscriber Manager for MPLS/VPN identification.
- Enable IP ranges.

How to Configure the Subscriber Manager for MPLS/VPN Support

Add this 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 Subscriber Manager 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 be turned on only when necessary for troubleshooting and should always be turned off for normal operation of the system.

Add this 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 Subscriber Manager to Allow IP Ranges

To set up the Subscriber Manager to work with MPLS/VPN to enable the IP ranges, use the `support_ip_ranges` command in the configuration file.

Set the `support_ip_ranges` parameter in the `[Data Repository]` section of the `p3sm.cfg` configuration file to “yes” as follows:

```
support_ip_ranges=yes
```



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

5 Managing MPLS/VPN Support

This section explains how to manage MPLS/VPN support:

- [How to Manage MPLS/VPN Support via SNMP](#), page 19
- [How to Monitor MPLS/VPN Support via SCE Platform CLI](#), page 19
- [How to Manage MPLS/VPN Support via Subscriber Manager CLU](#), page 25

How to Manage 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 about MPLS/VPN auto-learning.

The objects in the `mplsVpnAutoLearnGrp` provide these information:

- Maximum number of mappings
- Allowed current number of mappings

For more information, see the “Proprietary MIB Reference” chapter of *Cisco SCE 2000 and SCE 1000 Software Configuration Guide* or the “Cisco Service Control MIBs” chapter in these software configuration guides:

- *Cisco SCE 8000 10GBE Software Configuration Guide*
- *Cisco SCE 8000 GBE Software Configuration Guide*

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 percent 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.

How to Monitor MPLS/VPN Support via SCE Platform CLI

The SCE platform CLI allows you to do these:

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

How to Display VPN-related Mappings

Use these Viewer commands to display subscriber mappings. These commands display these information:

- Mappings for a specified VPN
- Listing of all currently logged-in VPNs
- Listing of all subscribers mapped to an IP range on a specified VPN
- Number of subscribers mapped to an IP range on a specified VPN
- 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 the [How to Display the Name of the Subscriber Mapped to a Specified VPN](#), page 22.)

How to Display Mappings for a Specified VPN

This section consists of these subsections:

- [Options](#), page 20
- [Displaying Mappings for a Specified VPN: Examples](#), page 20

Options

This option is available:

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

At the SCE > prompt, enter **show interface linecard 0 VPN name vpn-name** and press Enter.

Displaying Mappings for a Specified VPN: Examples

This is an output of the **show interface linecard 0 VPN name vpn-name** 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
```

This is an output of **show interface linecard 0 VPN name vpn-name** 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
```

This is an output of **show interface linecard 0 VPN name vpn-name** command for an automatically created VLAN:

```
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:

At the SCE > prompt, enter **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

This section consists of these subsections:

- [Options, page 21](#)
- [Displaying Subscribers Mapped to an IP range on a Specified VPN: Example, page 21](#)

Options

These options are available:

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

At the SCE > prompt, enter `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 an IP range on a Specified VPN: Example

This is an example of using `show interface linecard 0 subscriber mapping included-in IP ip-range VPN vpn-name` command to display subscribers mapped to an IP range on a specific VPN:

```
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

This section consists of these subsections:

- [Options, page 21](#)
- [Displaying the Number of Subscribers Mapped to Range on a Specified VPN: Example, page 21](#)

Options

These options are available:

- **ip-range**—IP range for which to display mapped subscribers
- **vpn-name**—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.

At the SCE > prompt, enter `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

This is an example of using `show interface linecard 0 subscriber amount mapping included-in IP ip-range VPN vpn-name` command to display the number of subscribers mapped to range on a specific VPN:

```
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. This section consists of these subsections:

- [Displaying the Subscriber Mapped to a Specified VPN: Example 1, page 22](#)
- [Displaying the Subscriber Mapped to a Specified VPN: Example 2, page 22](#)



Note This command provides backward compatibility for MPLS/VPN subscriber configuration in SCOS versions earlier than Version 3.1.5.

At the SCE# prompt, enter `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

```
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

At the SCE# prompt, enter `show interface linecard 0 MPLS/VPN non-VPN-mappings` and press Enter.

How to Clear Upstream VPN Mappings

Use the `clear interface linecard 0 VPN name vpn-name upstream mpls all` command, at SCE# prompt, to remove all learned upstream labels of a specified VPN.

This command, in effect, causes early label aging. Clearing the mappings allows relearning; labels are 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.

Options

This option is available:

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

How to Monitor Subscriber Counters

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

- [About Subscriber Counters, page 23](#)
- [Monitoring Subscriber Counters: Example, page 23](#)

About Subscriber Counters

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

- MPLS/VPN-based subscribers:
 - Current number of MPLS/VPN-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

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.

At the SCE# prompt, enter `show interface linecard 0 subscriber db counters` and press **Enter**.

Monitoring Subscriber Counters: Example

This is an example of how `interface linecard 0 subscriber db counters` command output:

```
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
```

How to Monitor MPLS/VPN Counters

Use this Viewer command to display MPLS/VPN information:

At the SCE# prompt, enter `show interface linecard 0 mpls vpn` and press **Enter**.

Monitoring MPLS/VPN Counters: Example

This is an example of the `show interface linecard 0 mpls vpn` command output:

```
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
```

How to Monitor the PE Routers

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

- Currently defined PE routers.
- Specified PE router.

How to Display the Configuration of all Currently Defined PE Routers

At the SCE# prompt, enter `show interface linecard 0 MPLS VPN PE-Database` and press Enter.

How to Display the Configuration of a Specified PE Router

At the SCE# prompt, enter `show interface linecard 0 MPLS VPN PE-Database PE-ID pe-id` and press Enter.

How to Monitor Bypassed VPNs

This section consists of these subsections:

- [How to Display the Currently Bypassed VPNs, page 24](#)
- [How to Remove all Learned Bypassed VPNs, page 24](#)

How to Display the Currently Bypassed VPNs

At the SCE# prompt, enter `show interface linecard 0 MPLS VPN Bypassed-VPNs` and press Enter.

How to Remove all Learned Bypassed VPNs

At the SCE# prompt, enter `clear interface linecard 0 MPLS VPN Bypassed-VPNs` and press Enter.

How to Monitor Non-VPN Mappings

- [How to Display Non-VPN Mappings, page 24](#)
- [How to Remove all Learned Non-VPN Mappings, page 24](#)

How to Display Non-VPN Mappings

At the SCE# prompt, enter `show interface linecard 0 MPLS VPN non-VPN-mappings` and press Enter.

How to Remove all Learned Non-VPN Mappings

At the SCE# prompt, enter `clear interface linecard 0 MPLS VPN non-VPN-mappings` and press Enter.

How to Manage MPLS/VPN Support via Subscriber Manager CLU

The Subscriber Manager CLU allows you to do these:

- 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, page 25](#)
- [How to Add a New MPLS-Based VPN, page 25](#)
- [How to Remove a VPN, page 25](#)
- [How to Display VPN Information, page 25](#)
- [How to Manage VPN Mappings, page 26](#)

Options

These options are available:

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



Note The RD may be specified rather than the route target.

- **PE-IP**—Loopback IP of the PE router connected to that VPN.

How to Add a New MPLS-Based VPN

At the shell prompt, enter the `p3vpn --add --vpn=VPN-Name --MPLS/VPN=RT@PE,(RT@PE2, RT@PE3,...)` command.

How to Remove a VPN

At the shell prompt, enter the `p3vpn --remove --vpn=VPN-Name` command.

How to Display VPN Information

This section consists of these subsections:

- [Listing All Existing VPNs, page 25](#)
- [Listing All Subscribers for a Specified VPN, page 25](#)
- [Displaying the Mappings for a Specified VPN, page 26](#)

Listing All Existing VPNs

At the shell prompt, enter the `p3vpn --show-all` command.

Listing All Subscribers for a Specified VPN

At the shell prompt, enter the `p3vpn --show-sub --vpn=VPN-Name` command.

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
```

Displaying the Mappings for a Specified VPN

At the shell prompt, enter the following `p3vpn --show --vpn=VPN-Name` command.

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

This section consists of these subsections:

- [Removing All Existing Mappings from a Specified VPN, page 26](#)
- [Removing a Specified Mapping from a Specified VPN, page 26](#)

Removing All Existing Mappings from a Specified VPN

At the shell prompt, enter the `p3vpn --remove-all-mappings --vpn=VPN-Name` command.

Removing a Specified Mapping from a Specified VPN

From the shell prompt, enter the `p3vpn --remove-mappings --vpn=VPN-Name --MPLS/VPN=RT@PE,(RT@PE2, RT@PE3,...)` command.

How to Add Mappings to VPN-Based Subscribers

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

- Set of IP addresses defined as `IP@VPN`.
- 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`).
- IP addresses of a CE router, defined by a `AS:value@VPN-NAME` (BGP community).

How to Add IP Address Mappings

Options

These options are available:

- **SUB-NAME**—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**—IP address. This may be any of these:
 - Single IP address (*x.x.x.x*).
 - Single range of IP addresses (*x.x.x.x/y*).
 - List of IP addresses separated by commas (*x.x.x.x, y.y.y.y, z.z.z.z*).
 - 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 is assigned.

- **--additive-mappings**—Option to use to add the new mappings to any existing ones. (Without this option, any existing mappings are overwritten.)

At the shell prompt, enter the `p3subs -add --subscriber=SUB-NAME --ip=IP1[/RANGE][,...]@VPN-NAME [--additive-mappings]` command.

How to Add VPN-Based Mappings

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

Options

These options are available:

- **SUB-NAME**—Name of the subscriber to be associated with the specified community attribute.
- **VPN-NAME**—Name of the VPN to which the subscriber is 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.)

At the shell prompt, enter the `p3subs -add --subscriber=SUB-NAME --vpn=VPN-NAME [--additive-mappings]` command.

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 PE router or in the 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

These options are available:

- **SUB-NAME**—Name of the subscriber to be associated with the specified community attribute.
- **AS:value@VPN-NAME**—Community attribute to assign to the VPN:
 - **AS**—Autonomous system. Integer in the range from 0 to 65535 assigned by the network administrator.
 - **value**—Community attribute. Integer in the range from 0 to 65535 assigned by the network administrator.
 - **VPN-NAME**—Name of the VPN to which the community attribute is assigned.

At the shell prompt, enter the `p3subs -add --subscriber=SUB-NAME --community=AS:value@VPN-NAME` command.

How to Remove VPN Mappings from Subscribers

This section consists of these subsections:

- [Removing All Existing Mappings from a Specified Subscriber, page 27](#)
- [Removing a Specified IP Mapping from a Specified Subscriber, page 28](#)
- [Removing a Specified VPN Mapping from a Specified Subscriber, page 28](#)
- [Removing a Specified Community-based Mapping from a Specified Subscriber, page 28](#)

Removing All Existing Mappings from a Specified Subscriber

At the shell prompt, enter the `p3subs --remove-all-mappings --subscriber=SUB-NAME` command.

Removing a Specified IP Mapping from a Specified Subscriber

At the shell prompt, enter the `p3psubs --remove-mappings --subscriber=SUB-NAME --ip=IP1[/RANGE][,...]@VPN-NAME` command.

Removing a Specified VPN Mapping from a Specified Subscriber

At the shell prompt, enter the `p3psubs --remove-mappings --subscriber=SUB-NAME --vpn=VPN-NAME` command.

Removing a Specified Community-based Mapping from a Specified Subscriber

At the shell prompt, enter the `p3psubs --remove-mappings --subscriber=SUB-NAME --community=AS:value@VPN-NAME` command.

How to Monitor Subscriber MPLS/VPN Mappings

Use the `p3subs` utility to manage VPNs.

At the shell prompt, enter the `p3subs --show-all-mappings --subscriber=SUB-NAME` command.

6 Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2011 Cisco Systems, Inc. All rights reserved.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

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