CHAPTER 2

Cisco Service Control Subscriber Manager Overview

Revised: January 16, 2014

Introduction

This chapter describes the Cisco Service Control Subscriber Manager solution and the Cisco Service Control Subscriber Manager application. This chapter contains the following topics:

Information About the Cisco Service Control Subscriber Manager

The Cisco Service Control Subscriber Manager is middleware that provides subscriber information to one or multiple Cisco Service Control Engine (Cisco SCE) platforms. The Cisco Service Control Subscriber Manager process subscriber information two ways:

- Pre-stores subscriber data
- Serves as a stateful bridge between an authentication, authorization, and accounting (AAA) system or provisioning system and Cisco SCE platforms

The SCE platforms process subscriber-aware functions, subscriber reporting, and policy enforcement.

Some Cisco Service Control solutions can also operate without subscriber awareness:

- Subscriber-less—The Cisco SCE process control-level and link-level analysis functions.
- Anonymous subscriber—The Cisco SCE dynamically creates “anonymous” subscribers per IP address. The Cisco SCE can process user-defined IP address ranges to differentiate between anonymous subscriber policies.

- Static subscriber awareness—The Cisco SCESCE is aware of subscribers but the allocation of network IDs (mainly IP addresses) to subscribers is static.

In these three modes, the Cisco SCE platform processes all subscriber-related functions and Subscriber Manager is not required.

Note Service providers can configure the Subscriber Manager to operate singly or in a *cluster* of two Subscriber Manager nodes. A cluster of Subscriber Manager nodes enables fail-over and high availability. Most of the information in this chapter applies to either single Subscriber Manager or cluster Subscriber Manager topologies.

The "Subscriber Manager Failover" section on page 3-1 pertains only to Subscriber Manager nodes in a cluster.

Subscribers in the Cisco Service Control Solution

In the Cisco Service Control Solution, the SCE manages a subscriber on the access, or downstream, side of the topology. The core of the network is on the other side of the SCE. The SCE applies accounting and policies to a subscriber individually on the access side.

Information About Managing Subscribers

The Cisco Service Control Subscriber Manager addresses the following issues pertaining to dynamic subscriber awareness:

- Mapping—The Cisco SCE encounters flows with network IDs (IP addresses) that change dynamically. The Cisco SCE dynamically maps the network IDs to the subscriber IDs. The Subscriber Manager database contains the network IDs that map to the subscriber IDs. Maintaining the network IDs is the primary function of the Subscriber Manager.

  Cisco SCE subscriber mapping supports private IP addresses within a VPN in addition to pure IP addresses. See the "Information About Managing VPNs" section on page 2-6 for more information.
- Policy—The Cisco Service Control Subscriber Manager serves as a repository of policy information for each subscriber. A service provider can preconfigure policy information in the Subscriber Manager, or dynamically provision when it receives the mapping information.
- Capacity—The Cisco SCE might be required to process more subscribers than it can concurrently manage. In this case, the Subscriber Manager serves as an external repository for subscriber information, while only the online or active subscribers are introduced to the Cisco SCE.
- Location—The Subscriber Manager sends subscriber information only to the relevant Cisco SCE platforms, when such functionality is required. A service provider can manage the distribution of subscriber information by using the domain mechanism or the Pull mode (see the "Pull Mode" section on page 2-10).

The Cisco Service Control Subscriber Manager database (see the "Subscriber Manager Database" section on page 2-5) can function two ways:

- As the only source for subscriber information when the Cisco Service Control Subscriber Manager works in standalone mode.

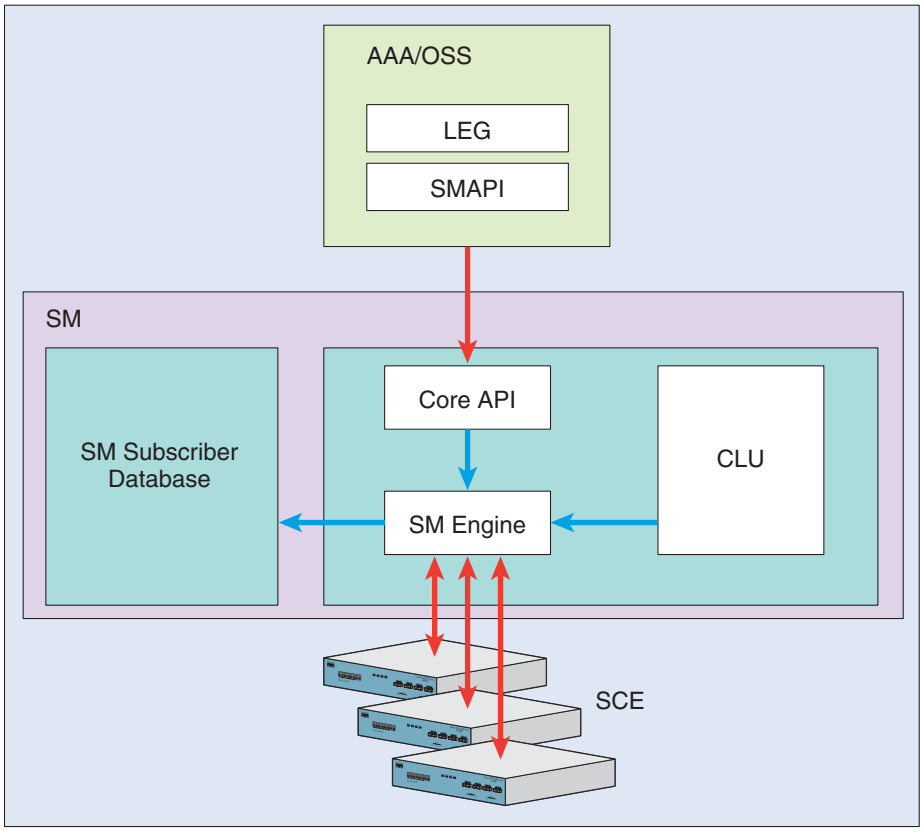
- As a cache of subscriber information when the Cisco Service Control Subscriber Manager serves as a bridge between a group of Cisco SCE devices and the customer AAA and Operational Support Systems (OSS).

This section contains the following sub-sections:

Flow of Subscriber Information

Figure 2-1 shows the flow of subscriber information through the Subscriber Manager.

Figure 2-1 Flow of Subscriber Information



The flow occurs as follows:

- Subscriber information enters the Cisco Service Control Subscriber Manager in one of two ways:
  - Automatically when the subscriber goes online—A service provider can use the Subscriber Manager Application Programming Interface (API) to integrate a Login Event Generator (LEG) with an AAA system (such as DHCP Server, RADIUS, or Network Access System [NAS]). The LEG identifies a subscriber login event and sends it to the Subscriber Manager.

  - Manual setup—A service provider imports subscriber information into the Subscriber Manager from a file or by using the Command-Line Utilities (CLU).
- Automatic and manual modes can be combined. For example, a service provider can manually load all subscribers into the Subscriber Manager and use the Subscriber Manager API to automatically change a subset of the subscriber records (domain, network ID, and so on).
- In automatic mode, the service provider can use the SCMS Subscriber Manager Java or C/C++ APIs to send subscriber information to the Subscriber Manager (see the *Cisco SCMS SM Java API Programming Guide* or the *Cisco SCMS SM C/C++ API Programming Guide*).
- The Subscriber Manager Engine performs the following actions:
  - Stores subscribers in the subscriber database
  - Introduces subscriber information to Cisco SCE
- The Subscriber Manager can pass information automatically to the SCE platform. Alternatively, the information can reside in the Subscriber Manager database until the SCE platform requests the information.

A service provider can configure a Subscriber Manager to interoperate with more than one SCE platform. The service provider can group these SCE platforms into domains. Each domain represents a group of SCE platforms that serve the same group of subscribers.

Number of Subscribers in the Cisco Service Control Subscriber Manager

A service provider can divide subscribers into the following logical types:

- Offline subscriber—A subscriber that currently does not have any IP address does not generate any IP traffic. Such subscribers are not stored in the SCE platform.
- Online subscriber—A subscriber that is currently online. At any particular time, a certain number of online subscribers are idle, that is, connected to the service provider but not generating any IP traffic.
- Active subscriber—An online subscriber that is generating IP traffic (for example, by browsing the Internet or downloading a file).

In addition, the total number of subscribers is comprised by all subscribers whose IP traffic might be traversing the SCE platforms in a specific deployment.

A service provider can deploy SCEs in four scenarios:

- The total number of subscribers can be statically stored in a single SCE platform.

  This is the simplest, most reliable scenario. It might not require the use of the Subscriber Manager.
- The total number of subscribers exceeds the capacity of the SCE platform. However, the number of online subscribers predicted at any time can be stored statically in the SCE platform.

  In this case, Subscriber Manager should be in Push mode. See the "Push Mode" section on page 2-10.
- The number of online subscribers exceeds the capacity of the SCE platform. However, the number of active subscribers predicted at any one time can be stored statically in the SCE platform.

  The Subscriber Manager must be used in Pull mode. See "Pull Mode" section on page 2-10.
- The number of active subscribers predicted at any one time exceeds the capacity of the SCE platform.

In this case, the service provider must install multiple SCE devices to divide the subscribers among the SCE platforms. If the system is divided into domains (see "Subscriber Domains" section on page 2-13.) The service provider can use Push mode to enable the Subscriber Manager to know in advance the SCE platform to which a particular subscriber should be sent. Otherwise, Pull mode is required.

For specific scenarios in which the service provider should deploy the Subscriber Manager with multiple servers and/or SCE platforms, see the "System Configuration Examples" section on page 5-8.

Note The SCE 2000 platform can store 200,000 subscribers, the SCE 8000 platform can store 1,000,000 subscribers.

Subscriber Manager Database

The Subscriber Manager uses a relational database from TimesTen, optimized for high performance and with a background persistency scheme. The In-Memory Database stores and retrieves subscriber records.

A subscriber record stored in the Subscriber Manager Database consists of the following components:

- Subscriber name (key)—A string that identifies the subscriber in the Subscriber Manager. Maximum length: 64 characters. This can be case-sensitive or case-insensitive depending on the configuration file. By default, the database is case-sensitive. If the database is case-insensitive, the Subscriber Manager converts the name to lower case when it updates or queries the database.
- Domain (secondary key)—A string that specifies which group of SCE devices processes the subscriber.
- Subscriber network IDs (mappings)—A list of network identifiers, such as IP addresses. The SCE uses these identifiers to associate network traffic with subscriber records.
- Subscriber policy—A list of properties that instruct the SCE what to do with the network traffic of a subscriber. The content of this list is application-specific.
- Subscriber state (for example, quota used)—A field that encodes the subscriber state recorded by the last SCE to process the network traffic of this subscriber.

A service provider can access the subscribers by using one of two indexes:

- Subscriber name
- Subscriber name + domain

Note We recommend that you do not open any connection to the Cisco Service Control Subscriber Manager Database directly, other than the Subscriber Manager process. Opening other connections impacts the Subscriber Manger process such as, uninstall, if the opened connection is not closed properly.

Note In cluster redundancy topology, the active machine database replicates the subscriber data to the standby machine database. For additional information, see Chapter 3, "Subscriber Manager Failover."

Subscriber ID

The Subscriber ID is a string representing a subscriber that is a unique identifier for each subscriber. For example, the Subscriber ID might represent a subscriber name or a cable modem MAC address.

The format rule for a Subscriber ID specifies that the ID can contain up to 64 printable characters. The ID is represented in ASCII code between 32 and 126 (inclusive), except for 34 (“), 39 ('), and 96 (`). The space character is allowed if it is not the last character (a trailing space) in the name.

For example:

```
String subID1=”xyz”;
String subID2=”xyz@abcdef.com”;
String subID3=”00-B0-D0-86-BB-F7”;
```

Information About Managing VPNs

A VPN is a named entity that a service provider can add to the Subscriber Manager and contains VPN mappings. A VPN can contain several MPLS/VPN mappings, or a single VLAN mapping. Subscribers that are part of a VPN do not contain VPN mappings directly, instead they contain a set of IP mappings of the form IP@VPN.

The Subscriber Manager addresses the following issues in allowing dynamic VPN awareness:

- Mapping—A set of MPLS-VPN mappings, or a single VLAN mapping.
  - A VLAN mapping comprises a simple VLAN-ID.
  - MPLS-VPN mappings are comprised of the Provider Edge (PE) router loopback IP address, the Route Target (RT) or Route Distinguisher (RD), downstream labels, and the IP ranges that correspond to the label.

Note A single VPN cannot hold both mapping types.

- Location—The Subscriber Manager supports sending VPN information only to the relevant SCE platforms, if this is required. This is implemented using the domain mechanism. The domain of a subscriber within a VPN must be identical to the domain of the VPN.

VPN entities are supported only when the Subscriber Manager is configured to work in “Push Mode.”

- Management of VPN with VLAN Network IDs, page 2-6
- Management of VPN with MPLS/VPN Network IDs, page 2-7
- Management of Subscribers with IP over VPN, page 2-7

Management of VPN with VLAN Network IDs

VPNs with VLAN network IDs are managed using one of the following methods:

- Statically—Using the Subscriber Manager CLU.
- Automatic creation of the VPN—When a network ID of the form IP@VLAN-Id is added to a subscriber with a VLAN-Id that does not exist in the Subscriber Manager, the Subscriber Manager automatically creates a VPN with the specified VLAN-Id. The VPN name is set to the VLAN-Id

value, and the VPN domain is set to the same domain as the subscriber. The benefit of this feature is that there is no need to manually configure VPNs with VLAN network IDs as they will be added automatically.

Management of VPN with MPLS/VPN Network IDs

VPNs with MPLS/VPN network IDs are managed using all of the following methods:

- Statically—Initially, the VPNs are added to the Subscriber Manager using their static information (that is the PE IP address, and the RT/RD values). This step is performed using the Subscriber Manager CLU.

  The notation used for the MPLS/VPN mappings is RT/RD@PE-IP. For example, 1000:1@10.10.10.10 represents a VPN with RT/RD 1000:1 of the PE router for which the loopback IP address is 10.10.10.10.

- Dynamically—The BGP LEG is then responsible for adding the dynamic VPN information (that is, the downstream label and its corresponding IP range). The dynamic information is added and removed in real-time according to the BGP updates in the network. Dynamic MPLS/VPN information is only added and stored in the Subscriber Manager database for VPNs that were configured statically during the previous stage.

The SCE only holds the downstream label and the PE IP for each VPN since it is the only information that is relevant for matching the flows to the subscribers. The RT/RD are used by the Subscriber Manager only to correctly correlate the VPN entity to the downstream labels.

Management of Subscribers with IP over VPN

A subscriber can possess one or more of the following network ID specifications:

- IP@VPN-name—The IP can be a single IP or an IP range.

  Overlapping IP ranges within a VPN are allowed. Mapping of a range to a subscriber is based on the longest prefix match.

- Community@VPN-name (MPLS/VPN only)—This network ID is used to automatically add IP ranges to subscribers (customer edge as subscriber mode).

Subscribers with IP over VPN are managed using one of the following methods:

- Statically—Using the Subscriber Manager CLU
- Dynamically—Using the RADIUS listener, or the Subscriber Manager API

Subscribers with communities over VPN are used to manage the traffic of a specific customer edge router of an MPLS/VPN network. The BGP community field is used to correlate the IP routes with the customer edge router. The subscriber is configured with a list of communities within the VPN using the syntax ‘community@VPN’. When the BGP LEG analyzes the BGP session, it also extracts the community field and adds all the IP routes in the BGP message to the subscriber that contains the same community field.

For example, suppose the following subscriber and VPN are configured in the Subscriber Manager:

- VPN—vpn1 with mappings 1000:1@10.10.10.10
- Subscriber—sub1 with mappings 100:100@vpn1

If a BGP update is received for VPN 1000:1@10.10.10.10 with label 10 and IP range 1.1.1.0/24, the BGP LEG adds label 10 to the mappings of vpn1, and the IP range 1.1.1.0/24@vpn1 to the mappings of sub1. The Subscriber Manager updates the SCE with the new MPLS label 10 of vpn1, and the new IP range 1.1.1.0/24 of sub1.

A subscriber can possess an IP@VPN network ID and a community@VPN network ID at the same time.

Information About Subscriber Manager Fundamentals

This section consists of these topics:

Subscriber Manager API

Use the Subscriber Manager API for:

- Altering the fields of an existing subscriber record
- Setting up new subscribers in the Subscriber Manager
- Performing queries

The Subscriber Manager API is provided in C, C++, and Java. It serves as the bottom-most layer of every LEG.

Subscriber Manager API programmer references are provided in the *Cisco SCMS SM C/C++ API Programmer Guide* and the *Cisco SCMS SM Java API Programmer Guide*.

Subscriber Manager Login Event Generators

A service provider can use the Subscriber Manager API to create Subscriber Manager Login Event Generators (LEGs). LEGs generate subscriber-record update messages (such as login/logout) and send them to the Subscriber Manager. A service provider usually installs LEGs with AAA/OSS platforms, or with provisioning systems. LEGs translate events generated by these systems to Cisco Service Control subscriber update events.

The unique functionality of each LEG depends on the specific software package with which it interacts. For example, RADIUS LEGs, DHCP LEGs, or some provisioning third-party system LEGs might be implemented. LEGs can set up subscribers or alter any of the fields of an existing subscriber record.

A service provider can connect multiple LEGs to a single Subscriber Manager. Alternatively, a single LEG can generate events for multiple domains.

Information About Subscriber Introduction Modes

As illustrated in Figure 2-1, the Subscriber Manager introduces subscriber data to the SCE platforms. This operation functions in one of two modes:

- Push—This is the simpler and recommended mode.

- Pull—Use this mode only in special cases, as explained below.

Push or Pull mode is configured for the entire Subscriber Manager system.

For information detailing the configuration of the subscriber integration modes, see the "Subscriber Manager General Section" section on page A-2.

- Push Mode, page 2-10
- Pull Mode, page 2-10

Push Mode

In the Push mode, immediately after adding or changing a subscriber record, the Subscriber Manager distributes, or *pushes*, this information to the relevant Cisco SCE platforms, as determined by the subscriber domain. When the subscriber starts transmitting traffic through the Cisco SCE platform, the Cisco SCE has the required subscriber information.

In the Push mode with IPv6 subscribers, the Subscriber Manager updates the Cisco SCE with the 64-bit IPv6 prefix as subscriber mappings.

In some scenarios, factors such as capacity limitations make it impossible to use the Push mode.

Note Use the Push mode only if all the online subscribers associated with a domain can be loaded simultaneously into all the Cisco SCE platforms in the domain.

Pull Mode

In Pull mode, the SCE platforms are not notified in advance of subscriber information. When an SCE platform cannot associate the IP traffic with a subscriber, it will request, or *pull*, the information from the Subscriber Manager.

The advantage of Pull mode is that there is no need to know in advance which SCE platform serves particular subscribers.

Pull mode has the following disadvantages:

- Increased communication in the Subscriber Manager-SCE link
- Increased load on the Subscriber Manager, as it processes incoming requests from both the SCE device and the LEG.

Note By default, the SCE does not request subscriber information from the Subscriber Manager. You must configure anonymous groups in the SCE for the set of IP ranges that should be requested from the Subscriber Manager. See the SCE User Guide for more details on anonymous subscriber groups.

Note You must use Pull mode when all online subscribers that are associated with a domain exceed the capacity of the SCE platforms in the domain. The number of active subscribers can still be loaded into the SCE platforms in the domain.

In the Pull mode with IPv6 subscribers, the IPv6 prefix information is learned using the Framed-IPv6-Prefix RADIUS attribute from the traffic via Cisco SCE. The details are updated in the Cisco Service Control Subscriber Manager database. When a flow from the corresponding user is detected in a Cisco SCE, a pull request is sent with the subscriber IP address to the Subscriber Manager.

The Cisco Service Control Subscriber Manager then checks for the IP Prefix that matches the IP address. If a match is found, the Cisco Service Control Subscriber Manager provisions the subscriber and prefix details to Cisco SCE. When another flow from a different IP is detected within the same prefix, Cisco SCE matches it to the right subscriber without contacting Cisco Service Control Subscriber Manager. Since the Framed-IPv6-Prefix is a RADIUS attribute, if you remove the AAA/RADIUS server, you must remove this attribute as well.

Table 2-1 summarizes the differences between the Push mode and Pull mode.

Table 2-1 Differences Between the Push Mode and Pull Mode

Aspect of Use	Push Mode	Pull Mode
When to use	For simple provisioning of subscriber information in the SCE platform	For real-time, on-demand subscriber information retrieval Use in large-scale deployments: • When there is no way of knowing from the IP assignment process which SCE platform will serve a particular subscriber • When the required number of logged-in subscribers is greater than the number of concurrently active subscribers that the SCE platform can manage
Functional flow at access time	• Subscriber network login or access • From subscriber information to LEG to Subscriber Manager • From Subscriber Manager to the relevant SCE platforms	• Subscriber network login or access • From subscriber information to LEG to Subscriber Manager (maintained in the Subscriber Manager database) • When the subscriber starts producing traffic that traverses the SCE platform, SCE platform asks for the subscriber information • From Subscriber Manager (Subscriber Manager database) to SCE platform
Subscriber information at the SCE platform	SCE platform always has current subscriber information: • Immediate policy enforcement • Real-time system architecture	SCE gets subscriber information on demand

Dual-Stack Subscribers

For subscribers with IPv4 and IPv6 addresses assigned, the LEGs learn the IP mapping through one or multiple iterations.

A subscriber may have IPv6 prefix and IPv4 address mappings at the same time. So the IPv4 and IPv6 mappings might reach the Subscriber Manager from one LEG or from different LEGs.

Dual-Stack Push Mode

Subscriber mappings are pushed to Cisco SCE for IPv4 and IPv6 separately in different login events.

Dual-Stack Pull Mode

When a pull request is sent, the Cisco Service Control Subscriber Manager responds to Cisco SCE on the basis on the requested mapping type. The Pull request is sent separately for IPv4 and IPv6 for a dual-stack subscriber.

SCE Subscriber Synchronization

The Subscriber Manager includes a mechanism to ensure that the SCE platforms' subscriber information is synchronized with the information in the Subscriber Manager database. This mechanism is activated in the following cases:

- When the Subscriber Manager reconnects to the SCE platform and the standby SCE within the cascade pair is not synchronized.
- If specifically requested by user. See "The p3net Utility" section on page B-12.

SCE Quarantine

From Subscriber Manager version 3.1.0, the Subscriber Manager can put an SCE into a quarantine state. This action is taken in extreme cases when the Subscriber Manager automatically detects that the SCE has a problem and is causing back-pressure of login events to the Subscriber Manager. This action prevents the SCE from causing problems for the Subscriber Manager when managing subscriber information for all of the other SCEs in the network.

When the SCE is quarantined, the Subscriber Manager does the following:

- Disconnects from the SCE to allow the SCE to resolve the problem.

  Waits for the quarantine-timeout period (starting at a minute).
- After the timeout expires, the connection to the SCE is re-established and the SCE is put into a post-quarantine state for another ten minutes.

If another failure occurs within the post-quarantine-timeout period, the quarantine-timeout is doubled. The quarantine state transition is logged to the user log.

The **p3net --connect** CLU resets the quarantine state immediately.

Working with Cascade SCE Setups

From Subscriber Manager version 3.1.0, the Subscriber Manager manages cascaded SCEs as a cascade pair and not as two separate SCEs. The Subscriber Manager uses the ability of the SCE to duplicate the subscriber data between the SCEs by updating only the active SCE.

The Subscriber Manager connects to both SCEs but sends log in operations only to the active SCE. Similarly, the Subscriber Manager performs subscriber synchronization only with the active SCE.

The standby SCE learns about the subscribers from the active SCE, which allows stateful failover. The Subscriber Manager identifies a fail-over event and synchronizes the SCE that became active so that it will receive the most up-to-date subscriber information.

Subscriber Domains

The Subscriber Manager provides the option of partitioning SCE platforms and subscribers into subscriber domains.

The deployment of domains enables a single Subscriber Manager to manage several separate network sections, and to better control the transfer of subscriber information to the SCEs.

A subscriber domain is a group of SCE platforms that share a group of subscribers. The subscriber traffic can pass through any SCE platform in the domain. A subscriber can belong to only a single domain. Usually a single SCE platform serves an individual subscriber at a particular time.

Domains are managed differently in the Push and Pull modes:

- In Push mode, all subscribers in a subscriber domain are sent to all SCEs in the domain. The primary reason to place a number of SCE platforms in a single domain is for redundancy.
- In Pull mode, the pull requests are processed only for subscribers in the domain of the pulling SCE platform. In Pull mode, a single domain usually covers all subscribers.
- From Subscriber Manager version 3.1.0, a service provider can move subscribers between domains in a process known as automatic domain roaming. After receiving an update that an existing subscriber has switched domains, the Subscriber Manager does the following:
  - In Push mode, the subscriber is automatically logged out from the old domain and then logged in to the new domain.
  - In Pull mode, the subscriber is automatically logged out from the old domain.

Note Automatic domain roaming is not backward compatible with previous releases of Subscriber Manager.

By default, a system is configured with one subscriber domain called *subscribers*. When you add an SCE platform to the Subscriber Manager, the SCE is automatically added to this default domain, unless otherwise specified. Subscribers are also associated with the default subscriber domain, unless otherwise specified. To associate a subscriber with a different domain, first define the domain in the configuration file. Then explicitly specify the domain when adding the subscriber to the Subscriber Manager. To associate an SCE platform with a nondefault subscriber domain, edit and reload the configuration file. For more information, see Chapter 5, “Configuration and Management.”

Information About Communication Failures

A communication failure might occur either on the LEG-Subscriber Manager communication link or on the Subscriber Manager-SCE communication link. A communication failure might occur due to a network failure or because the SCE, Subscriber Manager, or LEG has failed. High availability and recovery from a Subscriber Manager failure are discussed in the “Subscriber Manager Cluster” section on page 2-15.

When configuring the system, consider three issues related to communication failures:

- Communication failure detection—Timeout after which a communication failure is announced.
- Communication failure handling—Action to take when communication on the link fails.
- Communication failure recovery—Action to take when communication on the link resumes.

Failure Detection Mechanism

One of two mechanisms detects a communication failure:

- Monitor the TCP socket connection state. All peers monitor.
- Use a keepalive mechanism at the PRPC protocol level.

Failure Handling Mechanism

There are two configuration options for managing communication failures:

- Ignore communication failures
- Erase the subscriber mappings in the database and start managing flows without subscriber awareness

Erasing the mappings in the database is useful when you want to avoid incorrect mappings of subscribers to IP addresses. Issue a request to clear all mappings upon failure.

Failure Recovery Mechanism

The Subscriber Manager recovers from communication failures by resynchronizing the SCE platform with the Subscriber Manager database.

Subscriber Manager Cluster

The Subscriber Manager supports high availability with Veritas Cluster Server (VCS) technology. In a high availability topology, the Subscriber Manager software runs on two machines, designated as the active machine and the standby machine. Subscriber data is continuously replicated from the active to the standby machine, which minimizes data loss in case the active Subscriber Manager fails. When the active machine fails, the standby machine discovers the failure and becomes active. For additional information, see Chapter 3, "Subscriber Manager Failover."

Quota Management

The Quota Manager is a component of the Subscriber Manager, which enables Service Control solution providers to manage subscriber quota. The Quota Manager controls Service Control Application for Broadband (SCA BB) quota functionality, and acts as an entry-level quota policy repository. For complete details, see the *Cisco Service Control Management Suite Quota Manager User Guide*.

Virtual Link Management

The Virtual Link Manager (VLM) is a component of the Subscriber Manager, which enables Service Control solution providers to monitor and control individual subscriber links separately. The VLM enables providers to create a single policy that contains the tier differentiated packages. Part of creating a policy includes establishing a number of virtual links and then assigning subscribers to the virtual links. For complete details, see the *Cisco Service Control for Managing Remote Cable MSO Links Solution Guide*.

Subscriber Manager Management

Subscriber Manager management includes configuration, fault management, logging management, and performance management.

Configure the Subscriber Manager using the following components:

- Configuration file (**p3sm.cfg**)—Sets all configuration parameters of the Subscriber Manager.

Note Changes that you make in the configuration file take effect only when you load the configuration file using the Command-Line Utilities (CLU) or when you restart the Subscriber Manager.

  For a detailed description of the configuration file, see Appendix A, "Configuration File Options."

- Command-Line Utilities (CLU)—Enables subscriber management and monitoring of the Subscriber Manager. CLU commands are shell tools that you can use to manage subscribers, install or update applications, retrieve the user log, and load an updated configuration file.

  For a complete description of the Command Line Utilities, see Appendix B, "Command-Line Utilities."

  You can invoke the CLU through a Telnet or Secure Shell (SSH) session to the platform that hosts the Subscriber Manager.

Examine the Subscriber Manager user log files for logging, fault, and performance management. The log file contains information about system events, failures, and periodic system performance reports.

Subscriber Manager Fail-Over

You can configure the Subscriber Manager to operate singly or in a cluster. Operating in a cluster topology provides features such as fail-over and high availability. For complete details, see Chapter 3, "Subscriber Manager Failover.".