CHAPTER 2

Subscriber Manager Overview

Revised: February 29, 2012, OL-21080-06

Introduction

This module describes the Subscriber Manager (SM) solution, the handling of subscribers, and the fundamentals and management of the SM application.

Information About the Subscriber Manager

The Subscriber Manager is a middleware software component that supplies subscriber information for multiple Service Control Engine (SCE) platforms in deployments where dynamic subscriber awareness is required. It does this in one of two ways:

- By pre-storing the subscriber information
- By serving as a stateful bridge between an Authentication, Authorization, and Accounting (AAA) system or a provisioning system and the SCE platforms

The SCE platforms use subscriber information to provide subscriber-aware functionality, per-subscriber reporting, and policy enforcement.

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

- Subscriber-less—Control-level and link-level analysis functions are provided at a global device resolution.
- Anonymous subscriber—The system dynamically creates “anonymous” subscribers per IP address. User-defined IP address ranges may then be used to differentiate between anonymous subscribers policies.
- Static subscriber awareness—Subscriber awareness is required, but allocation of network IDs (mainly IP addresses) to subscribers is static.

In these three modes, the SCE platform handles all subscriber-related functionality and an SM module is not required.

Note Starting with SM version 2.2, you can configure the SM to operate either with or without a cluster of two SM nodes. The added functionality when operating in a cluster topology provides powerful new features such as fail-over and high availability. The information in most of this module is applicable whether using a cluster or not. However, for clarity, information that is applicable only when using a cluster is presented in the "Subscriber Manager Fail-Over" section on page 3-1.

Subscribers in the Cisco Service Control Solution

A *subscriber* is defined as a managed entity on the subscriber side of the SCE platform, to which accounting and policy are applied individually. The subscriber side of the SCE platform is the side that points to the access or downstream part of the topology, as opposed to the network side of the SCE platform, which points to the core of the network.

Information About Handling Subscribers

The SM addresses the following issues in allowing dynamic subscriber awareness:

- Mapping—The SCE platform encounters flows with network IDs (IP addresses) that change dynamically, and it requires dynamic mapping between those network IDs and the subscriber IDs. The SM database contains the network IDs that map to the subscriber IDs. This is the main functionality of the SM. Starting with version 3.1.5, the subscriber mappings are enhanced to support private IP addresses within a VPN in addition to pure IP addresses. See the "Information About Handling VPNs" section on page 2-5 for more information.
- Policy—The SM serves as a repository of policy information for each subscriber. The policy information may be preconfigured to the SM, or dynamically provisioned when the mapping information is provided.
- Capacity—The SCE platform or platforms may need to handle (over time) more subscribers than they can concurrently hold. In this case, the SM serves as an external repository for subscriber information, while only the online or active subscribers are introduced to the SCE platform.
- Location—The SM supports the functionality of sending subscriber information only to the relevant SCE platforms, in case such functionality is required. This is implemented using the domains mechanism or the Pull mode (see the "Pull Mode" section on page 2-9).

The SM database (see the "SM Database" section on page 2-5) can function in one of two ways:

- As the only source for subscriber information when the SM works in standalone mode.
- As a subscriber information cache when the SM serves as a bridge between a group of SCE devices and the customer AAA and Operational Support Systems (OSS).

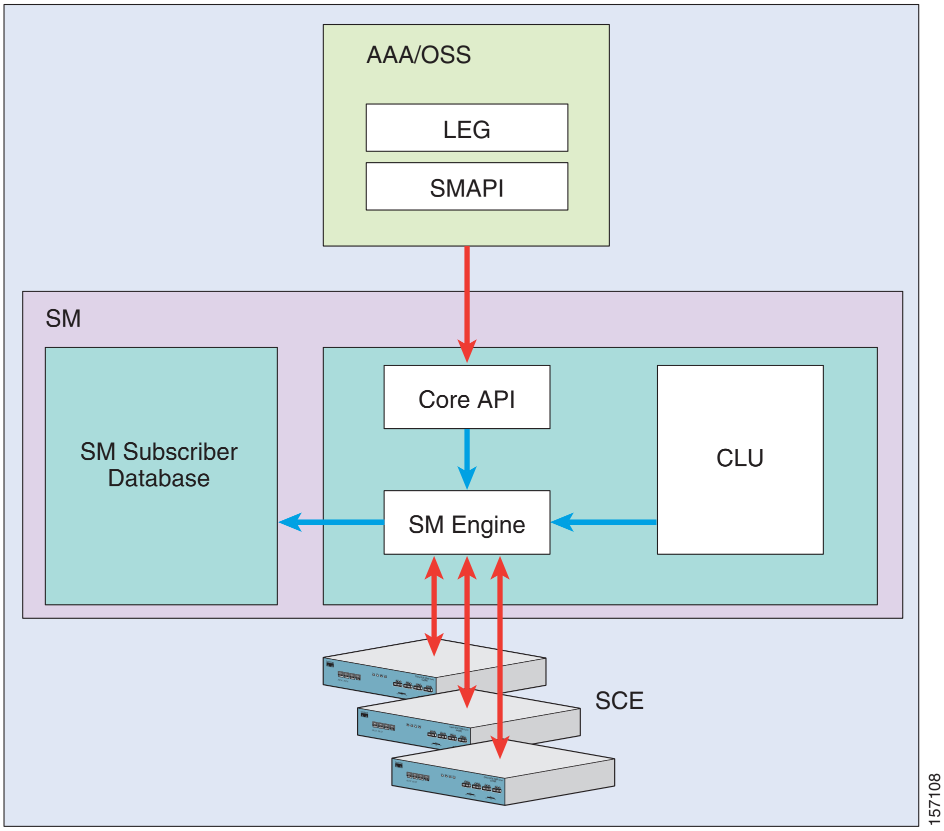
This section contains the following sub-sections:

- Flow of Subscriber Information, page 2-3
- Number of Subscribers in the SM, page 2-4
- SM Database, page 2-5
- Subscriber ID, page 2-5
- Information About Handling VPNs, page 2-5

Flow of Subscriber Information

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

Figure 2-1 Flow of Subscriber Information



The flow takes place as follows:

- Subscriber information enters the SM in one of two ways:
  - Automatically upon the subscriber going online—A Login Event Generator (LEG) software module that integrates with the customer AAA system (such as DHCP Server, RADIUS, or Network Access System [NAS]) identifies a subscriber login event, and sends it to the SM by using the SM Application Programming Interface (API).
  - Manual setup—Subscriber information is imported into the SM from a file or by using the Command-Line Utilities (CLU).
- Automatic and manual modes can be combined. For example, all subscribers may be loaded to the SM via manual setup, and a subset of the subscriber record (domain, network ID, and so on) changed automatically through the SM API.
- In automatic mode, the SCMS SM Java or C/C++ APIs are used for delegating subscriber information to the SM (see *Cisco SCMS SM Java API Programming Guide* or *Cisco SCMS SM C/C++ API Programming Guide*).

- The SM Engine:
  - Stores subscribers in the subscriber database
  - Introduces subscriber information to SCE Platforms
- The information may be passed automatically to the SCE platform, or it may reside in the SM database until the SCE platform requests the information.

The SM may be configured with more than one SCE platform. These SCE platforms may be grouped into domains. Each domain represents a group of SCE platforms that serve the same group of subscribers.

Number of Subscribers in the SM

The subscribers of the service provider may be divided into the following logical types (at any given moment):

- Offline subscriber—A subscriber that currently does not have any IP address and as such 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 will be idle, that is, connected to the service provider but not generating any IP traffic.
- Active subscriber—An online subscriber that is generating IP traffic (such as by browsing the Internet or downloading a file).

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

There are four general scenarios for a network system using the SCE platforms:

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

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

  It is recommended to use the SM in Push mode. See Push Mode, page 2-9.
- The number of online subscribers exceeds the capacity of the SCE platform, but the number of active subscribers predicted at any one time can be statically stored in the SCE platform.

  The SM must be used in Pull mode. See Pull Mode, page 2-9.
- The number of active subscribers predicted at any one time exceeds the capacity of the SCE platform.

  Multiple SCE devices must be installed to divide the subscribers among the SCE platforms. If the system is divided into domains (see Subscriber Domains, page 2-11), Push mode may be used so that the SM knows in advance to which SCE platform a particular subscriber should be sent. Otherwise, Pull mode is required.

For specific scenarios using the SM with multiple servers and/or SCE platforms, see System Configuration Examples, page 5-9.

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

SM Database

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

A subscriber record stored in the SM Database (SM-DB) consists of the following components:

- Subscriber name (key)—A string identifying the subscriber in the SM. 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 SM converts the name to lower case when updating or querying the database.
- Domain (secondary key)—A string that specifies which group of SCE devices handles this 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 this 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 handle the network traffic of this subscriber.

You can access the subscribers using one of two indexes:

- Subscriber name
- Subscriber name + domain

Note that in cluster redundancy topology, the active machine database replicates the subscriber data to the standby machine database. For additional information, see the Subscriber Manager Fail-Over module.

Subscriber ID

The Subscriber ID is a string representing a subscriber that is a unique identifier for each subscriber from the customer perspective. For example, it may represent a subscriber name or a CM MAC address. This section lists the formatting rules of a subscriber ID.

It can contain up to 64 characters. All printable characters with an ASCII code between 32 and 126 (inclusive) can be used, except for 34 (“), 39 ('), and 96 (`). The space character is allowed as long as it is not the last character in the name (trailing space).

For example:

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

Information About Handling VPNs

A VPN is a named entity that is added to the SM and contains VPN mappings. A VPN may 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 SM 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 SM supports sending VPN information only to the relevant SCE platforms, if this is required. This is implemented using the domains mechanism. The domain of a subscriber within a VPN must be identical to the VPN's domain.

VPN entities are supported only when the SM 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 2-6
- Management of Subscribers with IPs 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 SM 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 SM, the SM 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 SM using their static information (that is the PE IP address, and the RT/RD values). This step is performed using the SM 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 whose 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 SM 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 SM only to correctly correlate the VPN entity to the downstream labels.

Management of Subscribers with IPs over VPN

A subscriber can hold 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 (CE as subscriber mode).

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

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

Subscribers with communities over VPN are used to handle the traffic of a specific customer edge (CE) router of an MPLS/VPN network. The BGP community field is used to correlate the IP routes with the CE 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 SM:

- 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 SM 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 hold an IP@VPN network ID and a community@VPN network ID at the same time.

Information About SM Fundamentals

Subscriber Manager API

Use the SM API for:

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

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

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

SM Login Event Generators

The SM Login Event Generators (LEGs) are software components that use the SM API to generate subscriber-record update messages (such as login/logout) and send them to the SM. LEGs are usually installed with AAA/OSS platforms, or with provisioning systems. They 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 may be implemented. LEGs can set up subscribers or alter any of the fields of an existent subscriber record.

You can connect multiple LEGs to a single SM. Conversely, a single LEG can generate events for multiple domains.

Information About Subscriber Introduction Modes

As illustrated in Figure 2-1, the SM 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 SM system.

For information detailing the configuration of the subscriber integration modes, see SM General Section, page A-2.

- Push Mode, page 2-9
- Pull Mode, page 2-9

Push Mode

In Push mode, immediately after adding or changing a subscriber record, the SM distributes, or pushes, this information to the relevant SCE platforms, as determined by the subscriber domain. When the subscriber starts producing traffic through the SCE platform, it is ready with the required subscriber information.

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

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

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

The disadvantages of Pull mode are:

- Increased communication in the SM-SCE link
- Increased load on the SM, 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 SM. You must configure anonymous groups in the SCE for the set of IP ranges that should be requested from the SM. See the SCE User Guide for more details on anonymous subscriber groups.

Note Pull mode must be used when all online subscribers associated with a domain exceed the capacity of the SCE platforms in the domain (but the number of active subscribers can still be loaded into the SCE platforms in the domain).

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

Table 2-1 Differences Between Push Mode and Pull Mode

Aspect of Use	Push Mode	Pull Mode
When to use	For simple provisioning of subscriber information to the SCE platform	For real-time, on-demand subscriber information retrieval Used in large scale deployments: • When there is no way of knowing from the IP assignment process which SCE platform will be serving 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 handle
Functional flow at access time	• Subscriber network login or access • From subscriber information to LEG to SM • From SM to the relevant SCE platforms	• Subscriber network login or access • From subscriber information to LEG to SM (hold in the SM database) • When the subscriber starts producing traffic that traverses the SCE platform SCE platform asks for the subscriber information • From SM (SM 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

SCE Subscriber Synchronization

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

- When the SM reconnects to the SCE platform and the standby SCE within the cascade pair is not synchronized.
- If specifically requested by user. See Information About the p3net Utility, page B-13.

SCE Quarantine

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

When the SCE is quarantined, the SM 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 SM version 3.1.0, the SM handles cascaded SCEs as a cascade pair and not as two separate SCEs and utilizes the SCE's ability to duplicate the subscriber data between the SCEs by updating only the active SCE.

The SM connects to both SCEs but sends logon operations only to the active SCE. Similarly, the SM performs subscriber synchronization only with the active SCE.

The standby SCE learns about the subscribers from the active SCE, which allows stateful fail-over. The SM identifies a fail-over event and synchronizes the SCE that became active so that it will receive the most updated subscriber information.

Subscriber Domains

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

The motivation for the domains concept is to enable a single SM to handle several separate network sections, and for better control of subscriber introduction 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 a subscriber at any given time.

Domains are managed differently in the Push and Pull modes:

- In Push mode, all the subscribers in a subscriber domain are sent to all SCEs in the domain. The main reason for placing a number of SCE platforms in a single domain is for redundancy.
- In Pull mode, the pull requests are handled only for subscribers in the domain of the pulling SCE platform. In Pull mode, a single domain usually covers all the subscribers.

- From SM version 3.1.0, subscribers can be moved between domains in a process known as automatic domain roaming. After receiving an update that an existing subscriber has switched domains:
  - 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 SM behavior.

The system is configured with one default subscriber domain called *subscribers*. When adding an SCE platform to the SM, it is automatically added to this default domain, unless otherwise specified. Subscribers are also associated with this default subscriber domain, unless otherwise specified. To associate a subscriber with a different domain, first define this domain in the configuration file, and then explicitly specify it when adding the subscriber to the SM. To associate an SCE platform with a non-default subscriber domain, edit and reload the configuration file. For more information, see Configuration and Management, page 5-1.

Information About Communication Failures

A communication failure may occur either on the LEG-SM communication link or on the SM-SCE communication link. A communication failure may occur due to a network failure or because the SCE, SM, or LEG has failed. High availability and recovery from an SM failure are discussed in SM Cluster, page 2-13.

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

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

Failure Detection Mechanism

Either one of two mechanisms detects a communication failure:

- Monitoring the TCP socket connection state. All peers do the monitoring.
- Using a keep-alive mechanism at the PRPC protocol level.

Failure Handling Mechanism

There are two configuration options for handling communication failures:

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

Erasing the mappings in the database is useful when you want to avoid incorrect mappings of subscribers to IP addresses. This configuration is implemented by requesting to clear all mappings upon failure.

Failure Recovery Mechanism

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

SM Cluster

The SM supports high availability using the Veritas Cluster Server (VCS) technology. In a high availability topology, the SM 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, ensuring there is minimal data loss in case of active SM failure. When the active machine fails, the standby machine discovers the failure and becomes active. For additional information, see the Subscriber Manager Fail-Over module.

Quota Management

The Quota Manager (QM) is a component of the SM, which enables Service Control solution providers to manage, with a high degree of flexibility, 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 full details, see *Cisco Service Control Management Suite Quota Manager User Guide*.

Virtual Link Management

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

SM Management

SM management includes configuration, fault management, logging management, and performance management.

Configure the SM using the following:

- Configuration file (**p3sm.cfg**)—For setting 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 SM.

For a detailed description of this file, see Configuration File Options, page A-1.

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

  For a complete description of the Command Line Utilities, see Command Line Utilities, page B-1.

  The CLU can be invoked locally, through a Telnet (or secure shell [SSH]) session to the SM hosting platform.

Use the SM user log files for logging, fault, and performance management. The log file contains information regarding system events, failures, and periodic system performance reports.

Subscriber Manager Fail-Over

You can configure the SM to operate with or without a cluster. The added functionality when operating in a cluster topology provides powerful new features such as fail-over and high availability. For full details, see Subscriber Manager Fail-Over, page 3-1.