CHAPTER 1

Overview

This chapter describes the features and components in the Cisco Subscriber Edge Services Manager (Cisco SESM) Release 3.1(1) and Cisco Subscriber Policy Engine (Cisco SPE) Version 1.0. The chapter includes the following topics:

- SESM and SPE Product Descriptions, page 1-1
- Additional Required Network Software, page 1-5
- Key Features, page 1-8
- System Description and Network Diagram, page 1-11
- SESM in RADIUS Mode, page 1-13
- SESM in DESS Mode, page 1-15
- Software Component Descriptions, page 1-18

SESM and SPE Product Descriptions

This section introduces the SESM product. It includes the following topics:

- Introduction to SESM, page 1-1
- SESM Core Components, page 1-2
- Cisco Subscriber Policy Engine, page 1-2
- New World Service Provider Sample Application, page 1-3
- Captive Portal Sample Application, page 1-3
- Demo Installation, page 1-4
- SESM Deployment Modes, page 1-4
- J2EE and JMX Server Requirements, page 1-5

Introduction to SESM

The Cisco Subscriber Edge Services Manager (SESM) works in conjunction with other network components to provide extremely robust, highly scalable connection management to Internet services.

Internet service providers (ISPs) and network access providers (NAPs) deploy SESM to provide their subscribers with a web interface for accessing multiple Internet services. The ISPs and NAPs can customize and brand the content of the web pages and thereby control the user experience for different categories of subscribers.

SESM Core Components

SESM Release 3.1(1) is a solution composed of a number of applications built on a core set of software components. ISPs and NAPs can use these core components to further develop and customize SESM web applications, if required. The *Cisco Subscriber Edge Services Manager Web Developer Guide* describes how to develop SESM applications.

An SESM solution is deployed with the Cisco Service Selection Gateway (SSG), a Cisco IOS feature on the Cisco 6400 Universal Access Concentrator (UAC). Together, SESM and SSG provide subscriber authentication, service selection, and service connection capabilities to subscribers of Internet services.

Subscribers interact with an SESM web application using a standard Internet browser. They do not need to download any software or plug-ins to use the SESM web pages. After a subscriber successfully authenticates, the SESM web application presents a list of services that the subscriber is currently authorized to use. The subscriber can gain access to one or more of those services by selecting them from a web page. Alternatively, an automatic connection feature might provide automatic connection to services.

SESM Release 3.1(1) web applications deployed in Directory Enabled Service Selection/Subscription (DESS) mode incorporate the use of the Cisco Subscriber Policy Engine (SPE) Version 1.0. The SPE allows subscribers to perform account maintenance and self-care activities, such as subscribing to new services, creating subaccounts (for other members of the family, for example), and changing basic account information, such as address, phone number, and e-mail.

For subscribers of Internet services, an SESM web application offers flexibility and convenience, including the ability to access multiple services simultaneously.

For Internet service providers, an SESM web application provides a way to control the subscriber experience and promote customer loyalty. Service providers can change the look and feel of their SESM web application, brand the application, and control the content of the pages displayed to their subscribers.

Note The SESM product was previously called the Cisco Service Selection Dashboard (Cisco SSD).

Cisco Subscriber Policy Engine

The Cisco Subscriber Policy Engine (SPE) Version 1.0 is a policy server specifically customized to provide granular subscriber service policy. SPE combines role-based access control (RBAC) functionality with an open policy server. Service providers can create differentiated subscriber groups. Service and content providers can use the SPE to provide value added and differentiated services to the subscriber population.

SPE is installed when SESM Release 3.1(1) is deployed in DESS mode to provide the following enhanced features and capabilities:

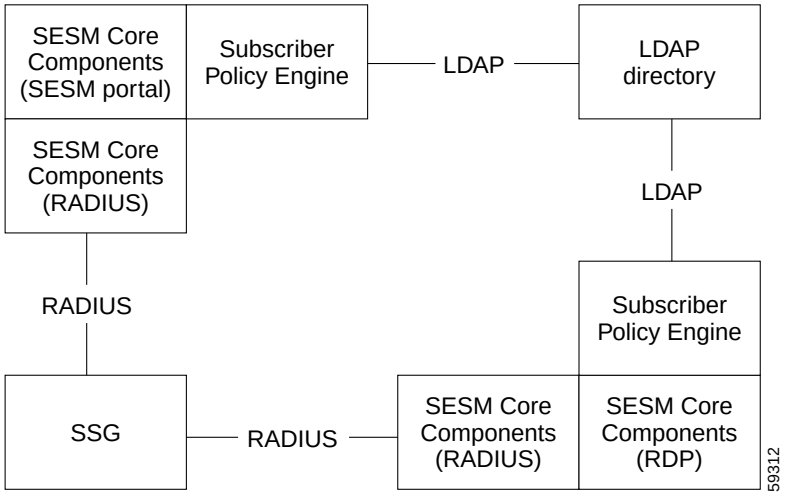
- Use of an LDAP directory to manage subscriber, service profile, and policy information
- Subscriber account self-care

- Subscriber sub-account management
- Subscriber self-subscription to services
- Bulk administration of large subscriber populations
- Delegated administration
- Allow service publishers and business partners access to service creation and management
- Allow service providers and business partners to publish services to targeted subscribers

In the SESM product and its documentation, the SPE components and features are called the DESS components and features.

Figure 1-1 shows the relationship between the SESM and SPE products.

Figure 1-1 SESM in DESS Mode Components



New World Service Provider Sample Application

The SESM installation package includes a sample SESM web application, called the New World Service Provider (NWSP), that you can configure and subsequently execute as an example of SESM capabilities. You can create the desired look-and-feel and branded aspects of a customized SESM application by altering the sample application or writing your own application using the NWSP as an example.

Captive Portal Sample Application

The SESM installation package includes a captive portal sample application. This application demonstrates how several powerful features in SESM Release 3.1(1) work together to redirect unauthenticated users to an SESM sign-on page immediately after they open a web browser. See the "Key Features" section on page 1-8 for more information about this and other SESM features.

Demo Installation

The SESM installation package provides an option to install the NWSP and captive portal sample applications in Demo mode. Demo mode simulates the actions of an SESM application without requiring additional network components. Demo mode is intended for demonstration purposes only and does not represent SESM performance in a production environment.

SESM Deployment Modes

The SESM Release 3.1(1) solution can be deployed in these modes:

- RADIUS deployment mode—This mode obtains subscriber and service profile information from a RADIUS server.
- DESS deployment mode—The Directory-Enabled Service Selection (DESS) mode integrates the Cisco Subscriber Policy Engine (SPE) Version 1.0 product with the SESM product to provide access to an LDAP compliant directory for subscriber and service profile information. SPE also provides enhanced functionality for SESM web applications and use of the role-based access control (RBAC) model to manage subscriber access.
- Demo mode—This mode demonstrates the capabilities of both RADIUS and DESS modes without requiring additional external components, such as SSG, a RADIUS server, or an LDAP directory server.

The SESM core model implements these modes in a plug-in style. Web developers use the same SESM application programming interface (API) to develop applications intended for either the RADIUS or the DESS modes. Applications intended for DESS mode deployment can include additional features provided by SPE. The *Cisco Subscriber Edge Services Manager Web Developer Guide* describes how to create applications for both RADIUS and DESS mode deployments.

The deployment option affects the following aspects of product installation and configuration:

- The SESM software components that you install and configure—The DESS deployment includes several additional software components to install and configure, all of which are included in the SESM installation package and described in this guide.
- The values of configuration parameters for the SESM software components.
- The network components that you are required to install, configure, and populate with subscriber and service profile information—The RADIUS mode requires SSG and a RADIUS server. The DESS mode requires SSG and an LDAP-compliant directory. Demo mode does not require any additional network components.

SESM Using an External RADIUS Server—RADIUS Mode

In a RADIUS deployment, a RADIUS server stores subscriber and service profiles. RADIUS refers to the Remote Dial-In User Service (RADIUS) database and server that performs authentication, authorization, and accounting (AAA) services for network connections. An SESM deployment works with any RADIUS server that accepts vendor-specific attributes (VSAs).

See the "SESM in RADIUS Mode" section on page 1-13 for more information about the components and data flow in a RADIUS mode deployment.

SESM Integrated with SPE—DESS Mode

In a DESS deployment, a directory stores subscriber and service profile information. The directory must be a Lightweight Directory Access Protocol (LDAP)-compliant directory.

A DESS deployment requires the Cisco Directory Enabled Service Selection/Subscription (DESS) component. You can install the DESS component from the SESM installation package if your SESM purchase license allows it. The DESS component is the Cisco Subscriber Policy Engine (SPE) Version 1.0, packaged for inclusion in the SESM product package.

See the "SESM in DESS Mode" section on page 1-15 for more information about the components and data flow in a DESS mode deployment.

J2EE and JMX Server Requirements

J2EE Server

SESM web applications are J2EE applications, requiring a J2EE-compliant server.

The NWSP sample application, configuration files, and startup scripts are configured to use the Jetty server components from Mort Bay Consulting. You can install the Jetty server using the SESM installation program. If desired, web developers at your site can deploy a J2EE-compliant server other than the Jetty server.

See the "Host Key Feature on SSG" section on page 1-6 before deploying a J2EE server other than the Jetty server.

JMX Server

SESM web applications require the services of a Java Management Extensions (JMX) server.

The installed NWSP sample application, the configuration files, and the startup scripts are set up to use the Sun example JMX server from Sun Microsystems. The SESM installation program installs the JMX server along with the Jetty server. If desired, web developers at your site can deploy a JMX-compliant server other than the Sun example server.

Additional Required Network Software

This section describes the network software that is required in an SESM deployment but is not provided by the SESM installation package.

- Cisco Service Selection Gateway, page 1-5
- Cisco Access Registrar or Third-Party RADIUS Server, page 1-6
- LDAP Directory, page 1-7

Cisco Service Selection Gateway

The Cisco Service Selection Gateway (SSG) is a software feature module embedded in Cisco IOS software running on the Cisco 6400 Universal Access Concentrator (UAC). Each node route processor on the Cisco 6400 UAC can host an SSG. The SSG configured with the Web Selection option works in conjunction with SESM.

SSG performs authentication and service connection tasks on behalf of an SESM application.

Required Cisco IOS Release

SESM Release 3.1(1) requires the SSG feature set embedded in Cisco IOS Release 12.1(5)DC1 or later. For information about this release of SSG, see the following documents.

- *Cisco 6400 Feature Guide*—This guide includes a chapter that documents SSG features.
- *Cisco 6400 Command Reference*—This guide includes a chapter that documents SSG configuration commands.
- *Cisco 6400 NRP—Release Notes for Cisco IOS Release 12.1(5)DC*

The "Related Documentation" section on page xiii provides URLs to the online location of these documents.

Communication Protocol

Regardless of the SESM deployment mode (RADIUS or DESS), SSG and an SESM web application communicate using the RADIUS protocol.

Host Key Feature on SSG

The host key is an important feature on the SSG. It uses a software token (or key) that uniquely identifies each subscriber on the host SSG currently logged on to SESM, even when multiple subscribers are using the same IP address. The host key feature also provides an SSG IP address in the key.

The host key feature provides the following advantages to SESM applications:

- Host key allows SESM applications to robustly handle overlapping IP addresses, nonroutable IP addresses, and dynamically assigned IP addresses.
- Host key eliminates the need to explicitly map subscriber subnets to SSGs.

Note The host key feature is planned for general availability in Cisco IOS Release 12.2(2)B.

When host key is enabled on the SSG, the SSG preserves the port number of the incoming HTTP request. This remote port number becomes the key that uniquely identifies each subscriber. The key is included in the request that is forwarded to the SESM web application.

The SSG makes the port number available, but the J2EE server must access this information and pass it along to the SESM web application. The Jetty server has been extended to allow access to the request handling part of the server API and thus get the remote port number. It does this with its PortBundleHandler. Therefore, only the Jetty server can support the host key feature.

Cisco Access Registrar or Third-Party RADIUS Server

The following scenarios require a RADIUS server:

- An SESM web application deployed in RADIUS mode—This deployment requires user and service profile information in a RADIUS database.
- An SESM web application deployed in DESS mode with an RDP running in Proxy Mode—This deployment requires user profiles in a RADIUS database. In Proxy mode, the RDP proxies authentication requests to a RADIUS database. RDP obtains service authorizations through DESS, based on the information in the directory.

- An SESM web application deployed in either mode when you want to use the SSG accounting features—For any SESM deployment, you can configure the SSG to generate accounting records and send them to a RADIUS server. The SSG accounting features are implemented independently from the SESM web application.

SESM works with any RADIUS server that accepts vendor-specific attributes (VSAs). The VSAs define the subscriber and service profile information required in the SESM deployment. The Cisco Access Registrar is a carrier class RADIUS platform that is fully tested with SESM. See the "Configuring Cisco Access Registrar for SESM Deployments" section on page D-11 for more information about using Cisco Access Registrar in SESM deployments.

Also see the following references for more information about configuring a RADIUS server in an SESM deployment:

- Appendix D, "Configuring RADIUS"—Describes the Cisco VSAs required in an SESM deployment. It also describes how to configure a RADIUS server for an SESM deployment.
- demo.txt file—Contains examples of subscriber and service profiles. This file is a MERIT flat file used by the NWSP sample application when it runs in Demo mode. The demo.txt file is included in your installation directory even if you do not specify demo mode at installation time. You can find demo.txt in the config directory under the nwsp directory (for example, nwsp/config/demo.txt).

LDAP Directory

An SESM web application deployed in DESS mode requires access to an LDAP-compliant directory. SESM is verified and officially supported to work with the Network Directory Service (NDS) eDirectory Version 8.5 from Novell, Inc. Although initial testing with the iPlanet Directory Server Version 5.0 indicates excellent results, Cisco has not fully verified it in an SESM deployment.

An LDAP directory allows interactive updates, a feature that is not supported by a RADIUS server. The DESS mode uses this update capability to offer SESM features that the RADIUS mode cannot provide, such as:

- Subscriber account self care features—Subscribers can change their account information and see those changes take effect immediately.
- Subscriber self subscription—Subscribers can subscribe to new services and have immediate access to the newly subscribed services.
- Sub-account creation—Subscribers can create sub-accounts to their main account and use the sub-accounts immediately.

Key Features

Table 1-1 describes the key features in SESM Release 3.1(1). For information about how to enable and configure these features, see Table 4-9 on page 4-42.

Table 1-1 Features in SESM Release 3.1(1) and SPE 1.0

Feature	Description
Multiple Internet service selection	An SESM web application provides a web portal from which subscribers can: • Authenticate or verify their identity • Select one or more services for connection • See which services are active in their current session and other session status information An SESM web application works in conjunction with SSG to authenticate the subscriber, to obtain the list of services that the subscriber is authorized to use, and to obtain session status information. The SESM application sends service connection requests to SSG, which makes the actual connection.
Java Server Pages (JSPs)	JSPs provide a standard way to integrate Java code with HTML to present interactive, dynamically updated, personalized, and branded web pages to your subscribers.
Walled gardens, open gardens, retail pages, and service advertisements	The following features are implemented through the use of customized JSPs: • Walled Gardens—Service providers can customize the look and feel of the walled garden presentation to subscribers by altering the JSPs. Walled gardens are the services available to a subscriber that require authentication. The specific services available to each subscriber are configured in subscriber profiles and are not affected by the JSPs. • Open Gardens—Service providers can use SESM to offer open gardens, branded offerings of value-added services that do not require authentication and might be specific to the service provider. Links to these services can appear on a pre-authentication page, or you can customize the post authentication pages to include the open gardens. • Retail Pages—Wholesale providers can offer retail pages with a customized look and feel for each Internet service provider. • Service Advertisement—Service providers can use SESM to reach subscribers with targeted messages and thereby increase the acceptance of new services.

Table 1-1 Features in SESM Release 3.1(1) and SPE 1.0 (continued)

Feature	Description
Captive portal	This feature works with the TCP redirect feature on the SSG to redirect HTTP requests for unauthenticated subscribers. • The TCP redirect feature on the SSG redirects incoming TCP packets to a specified SESM web application. With TCP redirect, service providers do not need to provide their subscribers with a URL to the SESM logon page. The subscribers are sent automatically to the logon page when they start a browser session. The TCP redirect feature in Cisco IOS Release 12.1(5)DC1 can redirect packets originating from unauthorized users, which, in effect, redirects packets from subscribers when they first open their Internet browsers and are not yet authenticated by SESM. Future releases will allow redirection based on the packet's source network or destination port. • If the SESM web application is running in captive portal mode, it has an associated captive portal application. The captive portal application: – Captures the original URL in the subscriber's request. For example, subscribers might have a home page setting, or they might open a browser and immediately enter a URL to a specific service or Internet reference page. (Original URLs are lost if you implement TCP redirect without captive portal.) – Redirects the browser to the authentication page of the main SESM application. – Includes the original URL in the redirect request, making this information available to the SESM web application. The NWSP sample application redirects the browser to the originally requested URL after successful authentication, thus honoring home page settings. You could customize your SESM web application to use this information in other ways.
Device and locale awareness	An SESM web application can detect a subscriber's preferred locale, device and browser type, and connection location and respond with web pages appropriate to the subscriber's preferred language, device capabilities, and connection type.
Single sign-on in a point-to-point (PPP) network	This feature offers a streamlined login procedure in a PPP network. A subscriber who logs on using a PPP client can access the SESM without having to re-enter the username and password.
Host key port bundle	This feature on the SSG ensures that each currently logged-on subscriber is uniquely identified, regardless of the IP address being used. This SSG feature allows SESM applications to support the following types of subscribers: • Overlapping IP addresses in PPP and bridged environments—SESM can differentiate between various subscribers using the same IP address. • Nonroutable subscriber IP addresses—SESM supports subscribers at sites using private IP addressing schemes, including subscribers of ISPs using private addressing schemes. • Dynamic IP address assignment—The subscriber session state status within SSG and SESM remains synchronized when a subscriber's IP address changes. This feature also enhances scaling and configuration of large SESM deployments.

Table 1-1 Features in SESM Release 3.1(1) and SPE 1.0 (continued)

Feature	Description
Highly scalable	An SESM web server application is highly scalable in the following ways: • SESM leverages the load-balancing features of J2EE technology. • When the SSG host key feature is enabled, SESM applications are completely stateless regarding subscriber sessions. SSG signals the SESM application whenever state changes occur. Therefore, the SESM applications can be started and stopped without affecting a subscriber. • The SSG host key port bundle feature simplifies large deployments because it eliminates manual mapping of subscriber subnets to SSGs.
The following features are provided by SPE and are available only when SESM is deployed in DESS mode.	
Subscriber account self care	This feature allows subscribers to change their own account details, such as address information and passwords. This subscriber updating capability relieves the service provider from time-consuming maintenance tasks. The NWSP sample application illustrates this feature.
Subscriber service subscription	This feature allows subscribers to subscribe to new services and have immediate access to those services. This feature relieves the service provider from time-consuming service enrollment tasks. It also benefits the subscriber because there is no delay in receiving access to a new service. Subscribers can also unsubscribe from a service. The NWSP sample application illustrates this feature.
Subscriber subaccount creation and management	This feature allows a subscriber with a main account to create subaccounts, with different services and access information in each subaccount. For example, a family might have subaccounts for each family member, with a different set of authorized services within each subaccount. The main account can create and delete subaccounts and subscribe to services for the subaccounts. The NWSP sample application illustrates this feature.
Cisco Distributed Administration Tool (CDAT)	CDAT is a web-based application for administrators to use in creating and maintaining the information on users, services, and access policy that is stored in an LDAP directory. The CDAT application is described in the *Cisco Distributed Administration Tool Guide*.
Role based access control (RBAC)	RBAC is an access model that allows administrators to manage groups of subscribers, rather than individuals. Using the RBAC model, administrators define roles, which have specific privileges, and groups, which have assigned roles. Individual subscribers are then assigned to a group and inherit the roles of that group. The Cisco DESS and AUTH APIs implement the RBAC model. See the *Cisco Distributed Administration Tool Guide* for more information about RBAC.

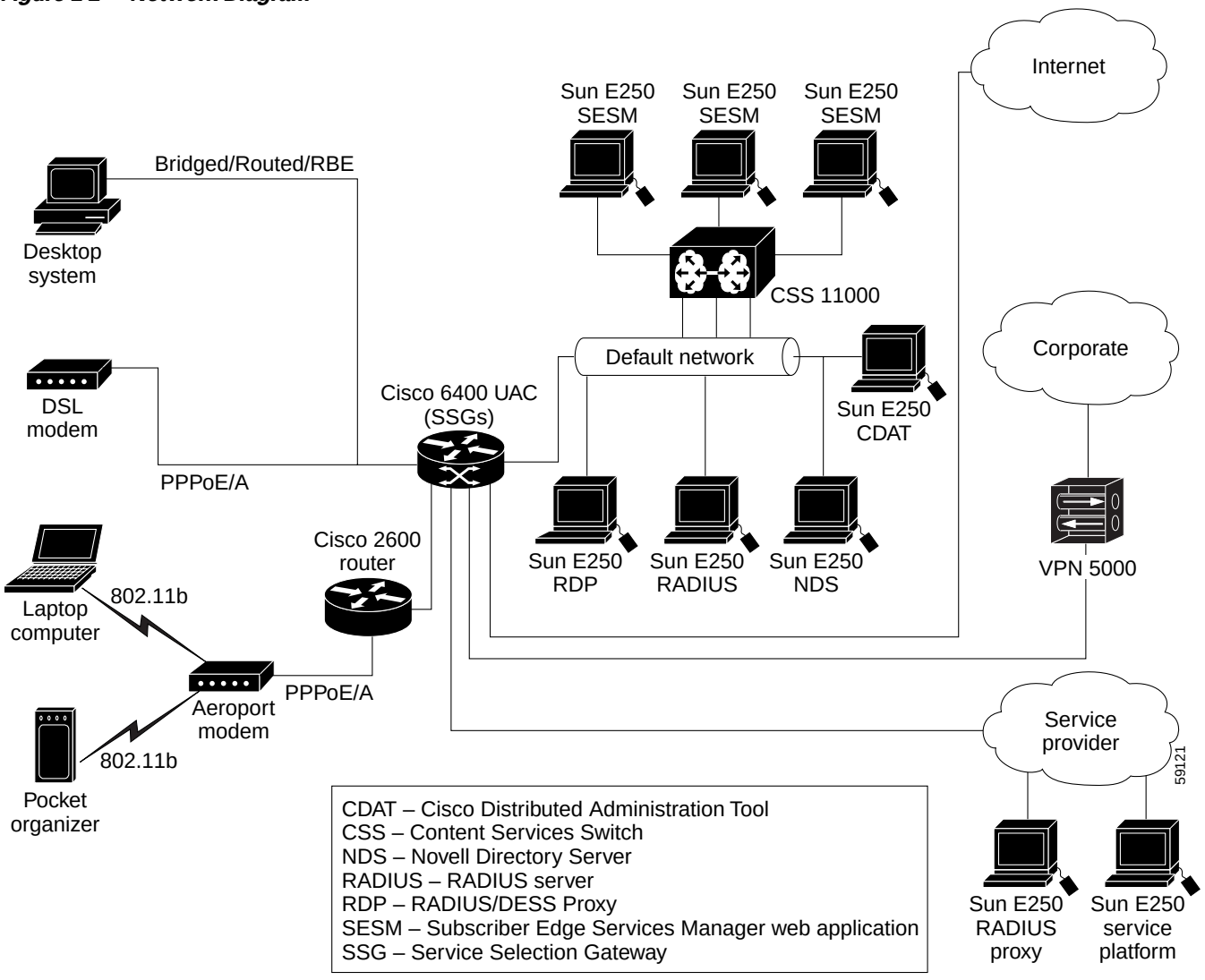
Accounting and Billing Features

The end-to-end solution offered by SESM applications provides support for accounting and billing based on actual services used and the duration of use. Accounting records are produced by a RADIUS server in response to SSG requests. See the SSG documentation for more information.

System Description and Network Diagram

Figure 1-2 shows an SESM deployment in an ISP or NAP communication network.

Figure 1-2 Network Diagram



Regardless of the type of modem or connection layer protocol a subscriber uses, all TCP packets are routed by the SSG when the SSG is enabled. The SSG is a feature in the Cisco IOS running on the node route processors (NRPs) on the Cisco 6400 UAC. Each NRP has an SSG separately enabled. Therefore, a typical production deployment includes multiple SSGs.

Physically, the TCP traffic passes through the SSG on its way to SESM. Logically the HTTP traffic goes directly to an SESM web application running on a default network. The *default network* is an IP address or subnet that TCP packets can access without authentication. The SESM web applications and their associated J2EE web servers run in this default network. The default network is configured on the SSG.

Production deployments might include multiple instances of J2EE web servers and associated SESM web applications on the default network. For production deployments, we recommend using enterprise-class server systems with hot-swappable components and load-balancing across the multiple

servers. The Domain Name System (DNS) resolves host names for any of the SESM web applications to the IP address of the load balancer. The Cisco Content Services Switch 11000 (CSS 11000) is preferred for load balancing.

The J2EE web servers receive the HTTP requests for the SESM web application. The SESM web application works with an SSG to establish a session for the user. SESM determines the IP address of the SSG that should handle the session as follows:

- If the host key feature is enabled on the SSG, the SSG's IP address is inserted in the packet. No explicit mapping of a client subnet to an SSG is required.
- If the host key feature is *not* enabled, configuration parameters in the web application's MBean configuration file map client subnets to specific SSGs.

An SESM Release 3.1(1) web application is highly scalable. You can start and stop instances of SESM web applications without affecting subscribers. This is because an SESM application is completely stateless. It does not store any subscriber session information. Rather, the SESM application queries SSG for session state information.

Connection Examples

This section describes how various access methods connect to an SESM web application.

Point-to-Point Protocol Example

This example describes the connection sequence for Point-to-Point Protocol (PPP) access to SESM. For example, consider a DSL subscriber using a PPP client configured on a laptop computer.

1. The subscriber launches the PPP client.
2. The TCP packet travels to the NRP on the Cisco 6400, which has SSG enabled.
3. The SSG on the NRP authenticates the PPP user.
4. The subscriber launches a web browser and sends an HTTP message.
   - If the SSG TCP redirect feature is configured, the subscriber can use any URL in the request, and will be automatically redirected to the SESM web application. If the captive portal feature is also configured, the subscriber could be redirected back to the original URL after being authenticated.
   - If the SSG TCP redirect is not configured, the subscriber must use the URL for the SESM web application.
5. The TCP packet containing the first HTTP request travels through the SSG, to the SSG's default network, to the J2EE web server and the SESM application.
6. If the SESM single sign-on feature for PPP subscribers is enabled, the user is already authenticated and SESM does not request an additional authentication. Rather, SESM queries the SSG for the subscriber's cached profile. A session is established, and SESM returns the subscriber's home page with a list of authorized services.
7. If the SESM single sign-on feature is disabled, or if PPP authentication failed in step 6, SESM returns the SESM logon page. When this request reaches an SESM web application, the application requests authentication services from the SSG. After the subscriber is authenticated, a session is established.

Routed Example

This example describes the connection sequence for a routed access to SESM, which includes the RFC1483 routed access method and the Routed Bridged Encapsulation (RBE) access method.

1. The subscriber launches a web browser and sends an HTTP message.
   - If the SSG TCP redirect feature is configured, the subscriber can use any URL in the request, and will be automatically redirected to the SESM web application. If the captive portal feature is also configured, the subscriber could be redirected back to the original URL after being authenticated.
   - If the SSG TCP redirect feature is not configured, the subscriber must use the URL for the SESM web application.
2. The TCP packet containing the first HTTP request travels through the SSG, to the SSG's default network, to the J2EE web server and the SESM application.
3. SESM returns the SESM logon page.
4. When SESM receives the subscriber's logon information, it requests authentication services from the SSG. After the subscriber is authenticated, a session is established.

SESM in RADIUS Mode

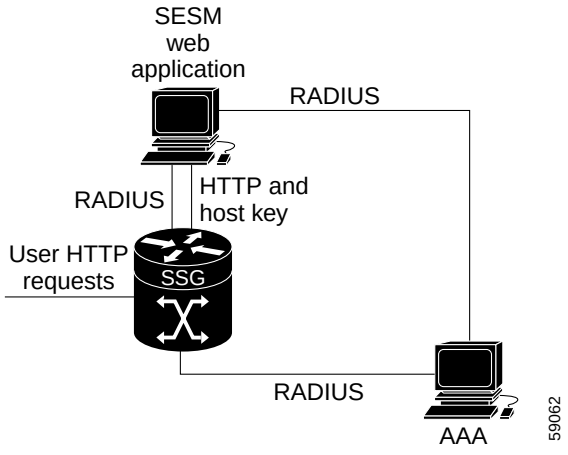
This section describes SESM deployment in RADIUS mode. It includes the following topics:

- Component Diagram for RADIUS Mode, page 1-13
- Processing a Subscriber Request in RADIUS Mode, page 1-14
- Installation and Configuration Requirements for RADIUS Mode, page 1-14

Component Diagram for RADIUS Mode

Figure 1-3 shows a simplified view of SESM deployed in RADIUS mode and the communication mechanisms used between the various software components.

Figure 1-3 SESM Deployed in RADIUS Mode



SSG and the SESM web application work together to process subscriber requests.

- SSG authenticates a subscriber based on a user profile stored in the AAA server.
- The SESM web application obtains the list of authorized services for a subscriber from the user profile in the AAA server.
- After the subscriber selects a service, SSG makes the connection to the service based on information in service profiles stored in the AAA server. In some cases, service preference information might be available in the user profile as well.

Processing a Subscriber Request in RADIUS Mode

Table 1-2 describes the role of SESM applications and SSG in processing typical subscriber actions in a RADIUS deployment.

Table 1-2 Role of Components in the a RADIUS Deployment

Subscriber Action	Software Activity	Components Involved
Subscriber logs on	Authenticate the subscriber in the system.	The SESM application initiates authentication by sending a message to SSG, using the RADIUS protocol. SSG forwards the RADIUS message to the RADIUS server. The RADIUS server authenticates the user and returns a message containing information from the subscriber's user profile. SSG creates an internal host object that represents the subscriber in the current session and forwards the message to SESM.
	Display web interface containing customized content appropriate for the logged on subscriber.	The RADIUS message contains the subscriber's user profile as stored in the RADIUS database. SESM can analyze the user profile and send appropriate content accordingly.
	Display the list of services that the subscriber is currently authorized to access.	The RADIUS message contains the list of services from the subscriber's profile. Authorization is implied for all services in the list. The SESM application obtains a service profile directly from the RADIUS server for each service in the list.
Subscriber selects a service	Access the service.	SESM sends a connection request to SSG. SSG creates a connection object, connecting the host object to the service. When the service is connected, SSG creates a service object. SSG then switches traffic from that subscriber to the requested service.
Subscriber selects a second service	Access a second service, without reauthentication.	The SESM application sends the request to the SSG. SSG creates a second connection object and service object. Both services are concurrently accessed.
Subscriber deselects a service	Stop access to the service.	The SESM application sends the request to the SSG. SSG destroys the appropriate connection object.

Installation and Configuration Requirements for RADIUS Mode

Table 1-3 summarizes the steps required to deploy SESM in RADIUS mode.

Table 1-3 Configuration Requirements for SESM in RADIUS Mode

Activity	Reference
1. Install and configure a RADIUS AAA server.	Appendix D, "Configuring RADIUS" and documentation from the RADIUS server vendor
2. Ensure that all Node Route Processors (NRPs) performing the SSG function are running Cisco IOS Release 12.1(5)DC1 or later.	*Cisco 6400 NRP—Release Notes for Cisco IOS Release 12.1(5)DC* [1]
3. Configure SSG. Use Cisco IOS commands on the SSG host to: – Configure SSG to listen for SESM requests – Enable or disable the host key mechanism – Set up SSG-to-RADIUS communication. – Configure security, routing, and other services provided by SSG.	Appendix B, "Configuring the SSG" *Cisco 6400 Command Reference Guide*[1]
4. Install and configure the SESM, which includes the NWSP sample application and a Jetty web server.	Chapter 3, "Installing Components"
5. Create user and service profiles in the RADIUS database.	Appendix D, "Configuring RADIUS" and documentation from the RADIUS server vendor

[1]See the "Related Documentation" section on page xiii for links to the online versions of these documents.

SESM in DESS Mode

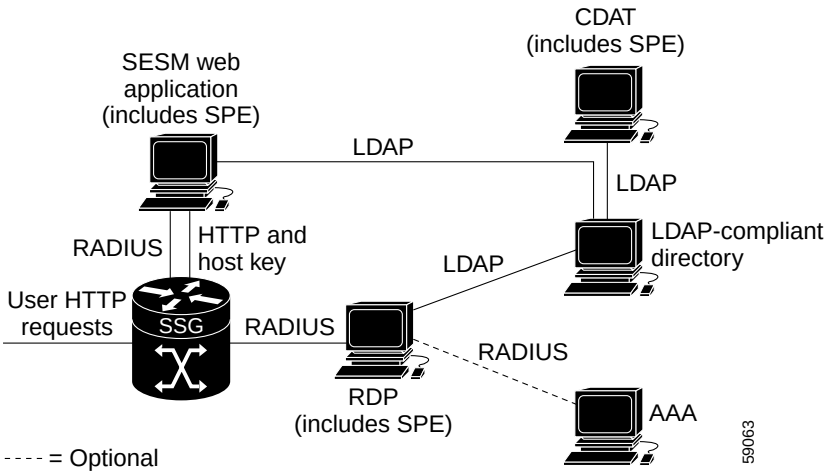
This section describes SESM deployment in DESS mode. It includes the following sections:

- Component Diagram for DESS Mode, page 1-16
- Processing a Subscriber Request in DESS Mode, page 1-16
- Installation and Configuration Requirements for DESS Mode, page 1-17

Component Diagram for DESS Mode

Figure 1-4 shows a simplified view of SESM deployed in DESS mode and the communication mechanisms used between the various software components.

Figure 1-4 SESM Deployed in DESS Mode



The optional AAA server might provide the following services:

- Accounting services
- User authentication services when RDP is configured in Proxy mode

In a DESS mode deployment, the Cisco Subscriber Policy Engine (SPE) Version 1.0 provides services to the SESM web application, CDAT, and RDP. To install SPE services, install the DESS component from the SESM installation package. This guide describes how to install and configure SPE to work with SESM components.

For more information about SPE, including its logical relationship to SESM components, see the "Cisco Subscriber Policy Engine" section on page 1-2.

Processing a Subscriber Request in DESS Mode

Table 1-4 describes the role of SESM applications and SSG in processing typical subscriber actions in a DESS deployment.

Table 1-4 Role of Components in a DESS Deployment

Subscriber Action	Software Activity	Components Involved
Subscriber logs on	Authenticate the user in the system.	The SESM application initiates authentication by sending a RADIUS message to SSG. SSG forwards the RADIUS message to the RDP. The RDP can authenticate using RADIUS or the LDAP directory, depending on how the RDP is configured: • If RDP is configured in proxy mode, it forwards the message to a RADIUS server. • Otherwise, RDP uses the DESS application programming interface (API) to forward the authentication request to the LDAP directory. The response is returned to the SESM application following the same path. SSG creates an internal host object that represents the subscriber in the current session.
	Display appropriate web pages to user.	After the subscriber is authenticated, the SESM application uses the DESS API to retrieve a user profile from the LDAP directory. The SESM application can analyze the profile and display appropriate web pages.
	Display the list of services in the subscriber's profile.	The SESM application uses the DESS API to retrieve service profiles from the LDAP directory for each service in the list.
Subscriber selects a service	Access the service.	SSG sends an authorization request to RDP. Regardless of the RDP mode, RDP always uses the DESS API to send service authorization requests to the LDAP directory. If the service is authorized, SSG creates an internal connection object, connecting the host object to the service. When the service is connected, SSG creates a service object. SSG then switches traffic from that subscriber to the requested service.
Subscriber selects a second service	Access a second service without reauthentication.	SSG sends another authorization request to RDP. Regardless of how it mode, RDP always uses the DESS API to send service authorization requests to the LDAP directory. If the service is authorized, SSG creates a second connection object and service object. Both services are concurrently accessed.
Subscriber updates an e-mail address	Update the LDAP directory.	The SESM application sends the update to the directory using the DESS API.
Subscriber creates a subaccount	Update the LDAP directory.	The SESM application sends the update to the directory using the DESS API.
Subscriber deselects a service	Terminate access to the service.	The SESM application sends the request to the SSG. SSG destroys the appropriate connection object.

Installation and Configuration Requirements for DESS Mode

Table 1-5 summarizes the installation and configuration activities for SESM in DESS mode.

Table 1-5 Configuration Activities Required for SESM in DESS Mode

Activity	Reference
1. (Optional) Install and configure a RADIUS server if: – You want to run RDP in Proxy mode so that it can authenticate subscribers using profiles in a RADIUS server, rather than in the directory. This option allows you to use existing RADIUS user profiles, rather than creating the information on the LDAP directory. (Service authorizations still occur using information in the directory.) – You want to use SSG accounting features.	Appendix D, "Configuring RADIUS" and documentation from the RADIUS server vendor
2. Ensure that all Node Route Processors (NRPs) performing the SSG function are running Cisco IOS Release 12.1(5)DC1 or later.	*Cisco 6400 NRP - Release Notes for Cisco IOS Release 12.1(5)DC* [1]
3. Configure SSG. Use SSG commands on the SSG host to: – Configure SSG to listen for SESM requests. – Set up SSG to RADIUS communication. – Enable the host key mechanism. – Configure security, routing, and other services provided by SSG.	Appendix B, "Configuring the SSG." *Cisco 6400 Command Reference Guide*[1]
4. Install and configure an LDAP directory. **Note** If you are using NDS, you must enable the cleartext password option.	Documentation from the directory vendor
5. Install and configure the SESM software components, which include: the NWSP sample application, Jetty web server, RDP, DESS, and CDAT.	Chapter 3, "Installing Components"
6. Create roles, groups, and user and service profiles in the LDAP directory.	*Cisco Distributed Administration Tool Guide*

[1]See the "Related Documentation" section on page xiii for links to the online versions of SSG documents.

Software Component Descriptions

This section describes the components that you can install from the SESM installation package.

- New World Service Provider, page 1-18
- Jetty Server, page 1-20
- Directory Enabled Service Selection, page 1-20
- RADIUS/DESS Proxy Server, page 1-21
- Cisco Distributed Administration Tool, page 1-21

New World Service Provider

When you install the NWSP component, the installation program prompts you to choose a deployment mode. The installation program then installs and configures software appropriate for that mode. In SESM Release 3.1(1), the modes are Demo mode, RADIUS mode, and DESS mode.

An installation of the NWSP component installs the following items:

- The NWSP sample application

- Captive portal sample application
- Images and JSPs for the NWSP application
- SESM core component class libraries
- API documentation for the SESM libraries
- Configuration and startup files for the NWSP sample application

The New World Service Provider (NWSP) is a sample SESM application. The first step towards developing a customized SESM application is to install and configure the NWSP application in a development environment. You can use this sample application as a starting point for creating a customized and branded SESM application.

See the *Cisco Subscriber Edge Services Manager Web Developer Guide* for information about developing a customized SESM application. Use the configuration information in Chapter 4, "Configuring Components after Installation," to deploy and configure the customized application.

The captive portal sample application demonstrates how several powerful features in this SESM release work together to redirect unauthorized users to an SESM sign-on page immediately after opening a web browser. With this feature, the service provider does not need to provide users with the URL to the SESM sign-on page.

SESM Sample Applications and Demos

This section defines the differences between a sample and a demo application.

SESM Sample Application

An SESM sample application is a fully functioning web application that was built using the SESM development library. It uses the services of the Jetty web server and the JMX management server. Before running the sample application, you need all other solution components installed and configured. For example, you need a fully configured SSG component running on a Cisco 6400 UAC. The RADIUS server (for RADIUS mode) or the LDAP-compliant directory (for the DESS mode) must be installed, configured, running, and populated with user and service information.

Demo Mode

The Demo mode is an SESM application running in a simulated network. The Demo runs without access to other solution components, such as SSG, RADIUS server, or LDAP directory. An SESM application running in standalone Demo mode is *only* intended for demonstration purposes. Demo mode is not in any way representative of Cisco SESM performance in an end-to-end solution with actual network components.

Note If you install the Demo mode, and then later want to perform some development on a customized SESM application, we recommend that you perform another installation. Otherwise, you will need to perform extensive edits to the MBean configuration files.

Demo mode simulates the actions of an SESM deployment in both RADIUS and DESS modes. It uses a local copy of a Merit RADIUS file to obtain profile information. See Chapter 2, "Demo Quick Start," for information about installing and using SESM in Demo mode.

Jetty Server

When you install the jetty component from the SESM installation package, you install the following items:

- Jetty web server—Jetty is a J2EE-compliant server package from Mort Bay Consulting that is released under an open source license. The license puts few restrictions on usage of Jetty. For more information about the Jetty server, see:

  http://jetty.mortbay.com/

- JSP engine—Jetty includes a Java Server Pages (JSP) package, which is currently the Jasper JSP engine from Apache Software Foundation.
- Sun example Java Management Extensions (JMX) server—This is a fully functional JMX server from Sun Microsystems. SESM depends on the JMX server for internal object configuration. For more information about JMX technology and its related JMX MBean standards, see:

  http://java.sun.com/products/JavaManagement

The NWSP application, CDAT, and RDP are installed with configuration files and startup scripts that are ready to run using the Jetty web server and the Sun example JMX server. However, SESM is designed to allow the use of any J2EE web server and any JMX-compliant server. An SESM web application, such as the NWSP sample application, requires an HTTP listener (web server) and a JMX server.

Note For SESM Release 3.1(1), the host key feature works only with a Jetty server.

Directory Enabled Service Selection

When you install the directory-enabled service selection (DESS) component from the SESM installation package, you install the following items:

- Cisco SPE AUTH library—The AUTH library implements a role-based access control (RBAC) authorization model. The RBAC model allows administrators to manage groups of subscribers, rather than individuals. Using the RBAC model, administrators define roles, which have specific privileges, and groups, which have assigned roles. Individual subscribers are then assigned to a group and inherit the roles of that group.
- Cisco SPE DESS library—The DESS library provides the framework for using the RBAC model in an LDAP directory.
- Files containing the directory schema extensions. The install program can optionally apply these extensions to your LDAP directory.
- Files containing sample RBAC data.

See the *Cisco Distributed Administration Tool Guide* for information about the RBAC model, the DESS and AUTH extensions to an LDAP directory, and how to develop subscriber and service profile information in the RBAC model.

RADIUS/DESS Proxy Server

The RADIUS/DESS Proxy (RDP) server is a RADIUS server that can proxy profile requests or use the DESS APIs to query the directory for profiles. RDP acts as the mediator between SSG, which communicates using RADIUS protocol messages, and the LDAP directory schema extensions, which require the DESS API for communication. RDP is a required component in the deployment of SESM in DESS mode.

You can configure the RDP to run in two modes:

- Default mode—In this mode, RDP queries the directory to obtain user authentication and service authorization.
- Proxy mode—In this mode, RDP sends user authentication requests to a specified RADIUS server, rather than to the LDAP directory. This option allows service providers with large RADIUS authentication and accounting services already deployed to continue to use the existing RADIUS database for authenticating users.

  This mode does not affect service authorizations. Regardless of the mode, RDP obtains all service authorizations from information in the LDAP directory.

RDP is a Java2 application that uses the services of a JMX server for configuration.

Cisco Distributed Administration Tool

The Cisco Distributed Administration Tool (CDAT) is an administrator's web-based interface for managing data in the DESS and AUTH extensions to the LDAP directory. CDAT provides the means for creating and maintaining users, services, user groups, service groups, roles, and policy rules for the RBAC model.

CDAT, a J2EE application, runs on a J2EE server and uses the services of a JMX server for configuration.

This guide describes how to install and configure CDAT. For information about using CDAT, creating profiles in the RBAC model, and the DESS and AUTH directory extensions, see the *Cisco Distributed Administration Tool Guide*.