SESM Solutions for Service Selection and Connection with SSG

This chapter describes SESM solutions for service selection and connection. These solutions work in conjunction with the Cisco Service Selection Gateway (SSG) for network access and connection management. These solutions can work with profiles stored on either a RADIUS database or LDAP directory.

This chapter includes the following topics:

Overview

For service selection and connection solutions, the Cisco Subscriber Edge Services Manager (SESM) works in conjunction with the Service Selection Gateway (SSG) to provide robust, highly scalable connection management to services in the broadband and mobile wireless markets. Internet service providers (ISPs) and network access providers (NAPs) deploy SESM to provide their subscribers with a web interface, or portal, for accessing multiple IP services.

This solution is deployed with the Cisco SSG, a feature set embedded in the Cisco IOS software broadband release train. Some of the devices on which SSG can run include the Cisco 7200 series high-performance multifunction router, the Cisco 7400 series router, and the Cisco 6400 Universal Access Concentrator (UAC).

The SESM applications run in a default network accessible to the SSG. Together, SESM and SSG provide subscriber authentication, service selection, and service connection capabilities to subscribers in the broadband and mobile wireless environments.

Subscribers interact with SESM web portals using a standard Internet browser. They do not need to download any software or plug-ins to use the SESM web portal. After a subscriber successfully authenticates, the SESM web portal 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 the web portal. Alternatively, an automatic connection feature can automatically connect subscribers to services after authentication.

Required Cisco IOS Release for SSG

Features in SESM Release 3.1(5) require the SSG embedded in the Cisco IOS Release 12.2(4)B or later. SESM Release 3.1(5) is backward compatible and is verified to work with previously released versions of the Cisco IOS broadband release train containing the SSG feature. For example, SESM Release 3.1(5) portals can be deployed with the SSG in Cisco IOS Release 12.1(3)DC running on the Cisco 6400 UAC.

For information about SSG in the Cisco IOS Release 12.2(4)B, see the following documents:

- *SSG Features in Release 12.2(4)B*—The online location of this document is:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_4/122b4_sg/

- Product documentation for the device on which SSG is running

SSG Platforms

The following platforms, when running the Cisco IOS Release 12.2.(4)B or later, with SSG enabled, are verified to work with SESM:

- Cisco 6400 Universal Access Concentrator (UAC). Each node route processor (NRP) on the Cisco 6400 UAC runs its own Cisco IOS software and can be an SSG platform.
- Cisco 7200 Series high-performance multifunction routers
- Cisco 7400 Series Internet routers

Communication Between SESM Applications and the SSG

SESM applications use command codes tunneled inside RADIUS requests to communicate with SSG. SSG distinguishes SESM requests from RADIUS requests by the presence of these command codes. SSG replies to SESM requests with either an access-accept or access-reject message.

Web Server Dependencies

Certain web server capabilities are required in SESM deployments that depend on the SSG TCP redirect feature or the port-bundle host key feature. Currently, the only web server that can provide the required capabilities is the Jetty server from Mort Bay Consulting. The rest of this section describes the dependency.

To support the above-mentioned features, SSG rewrites TCP packets destined to the default network, as follows:

- For the TCP redirect feature, SSG rewrites the destination port and IP address of the TCP packet
- For the port-bundle host key feature, SSG rewrites the source port and IP address of the TCP packet

The SSG rewrites only the TCP packet information; the corresponding values for the HTTP request contained in the TCP packet do not match. The SESM portal depends on the web server to access the socket-level values and add them to the HTTP request as request attributes. A special handler is required to perform this work. Currently, the Jetty server is the only J2EE-compliant web server that can perform this function.

Port-Bundle Host Key Feature on SSG

The port-bundle host key is an SSG feature that is important in SESM deployments. The port-bundle host key feature uses a software token (or key) that *uniquely* identifies each edge session on the SSG host, even when multiple subscribers are using the same IP address. The port-bundle host key feature also provides an SSG IP address in the key.

The port-bundle host key feature provides the following advantages to SESM portals:

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

When port-bundle host key is enabled on the SSG, SSG rewrites the source port number and IP address of TCP packets destined to the default network. The new source port and IP address combination becomes the key that uniquely identifies each session. The new IP address is the SSG IP address. The new port number identifies a specific edge session on the SSG.

System Description and Network Diagram

This section provides an overview of SESM deployment and how it fits into a network access provider (NAP) or Internet service provider (ISP) communication network.

Access Technologies

Subscribers can access the Cisco SESM portal over any access technology, including wireless LAN, fixed wireless, leased line, DSL, and GPRS, with any Web browser on a variety of devices, including Wireless Access Protocol (WAP) phones, personal digital assistants (PDAs), and desktops.

Default Networks

A *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 the default network. The default network is configured on the Service Selection Gateway (SSG).

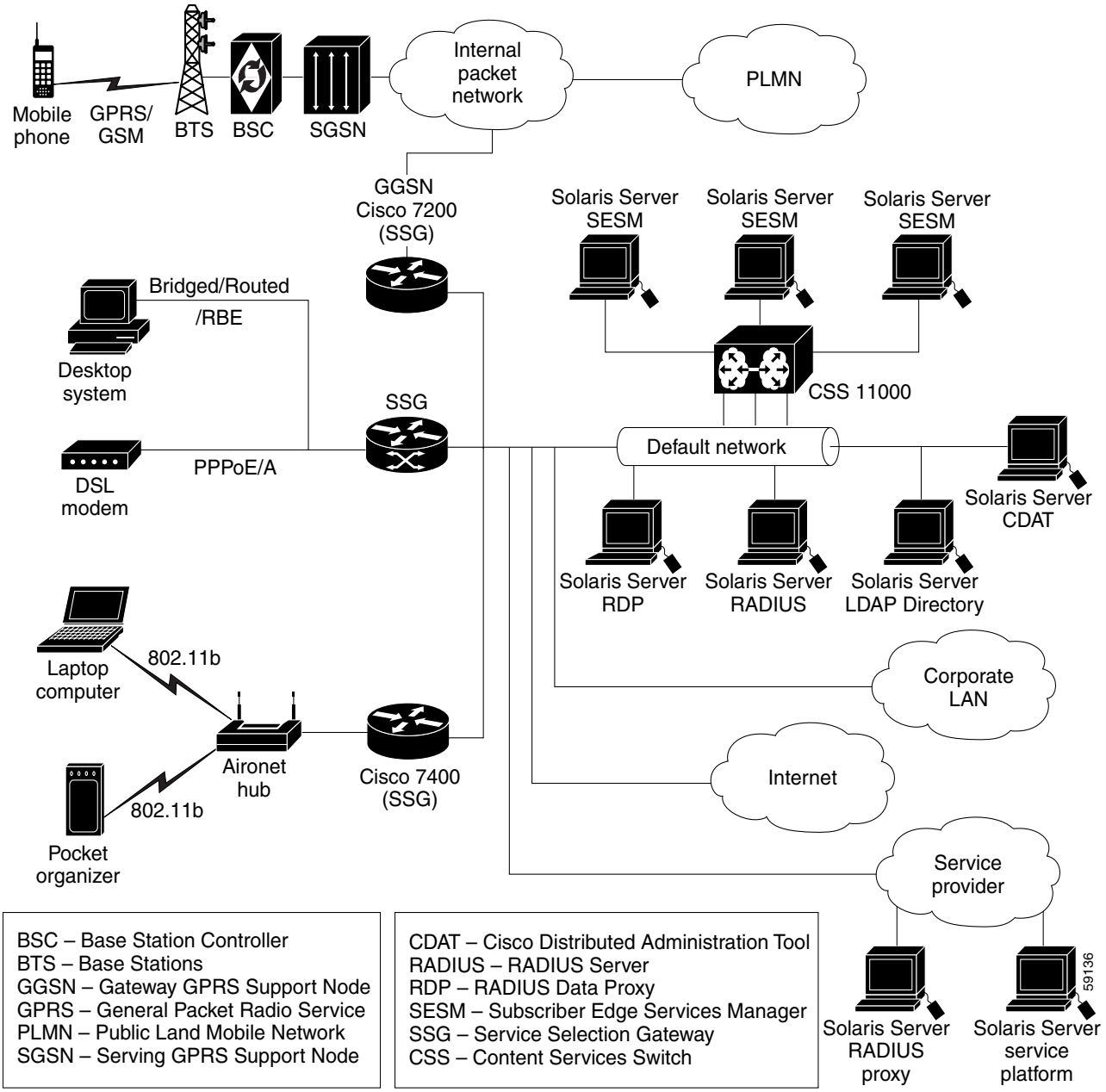
Service Selection Gateway

This SESM solution works with the Cisco Service Selection Gateway (SSG), a feature set embedded in the Cisco IOS broadband release train. Some of the devices on which the SSG can run include the Cisco 7200 Series high-performance multifunction router, the Cisco 7400 Series router, and the Cisco 6400 Universal Access Concentrator.

Network Diagram

Figure 3-1 is a conceptual network diagram showing SESM components, SSGs, and a default network. A typical deployment might consist of several routers of the same type, each one with its own default network, with SESM applications deployed on each of the default networks.

Figure 3-1 Network Diagram



Data Flow

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. Physically, the TCP traffic passes through the SSG on its way to SESM. Logically the HTTP traffic flows directly to the SESM portal application running on a default network.

J2EE web servers listen for HTTP requests for the SESM portal. The portal 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 port-bundle host key feature is enabled on the SSG, the SSG's IP address is inserted at the source IP address of the TCP packet.
- If the port-bundle host key feature is *not* enabled, configuration parameters map client subnets to specific SSGs.

Scaling and Load Balancing

SESM portal applications are highly scalable. You can start and stop instances of SESM portal applications without affecting subscribers. This is because the SESM portal application is completely stateless. It does not store any subscriber session information. Rather, the portal application queries SSG for session state information.

Production deployments might include multiple instances of J2EE web servers and associated SESM portals 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 portal applications to the IP address of the load balancer. The Cisco Content Services Switch 11000 (CSS 11000) is preferred for load balancing.

Connection Examples

This section provides some examples of how a subscriber gains access to SESM portals.

Example Using the Point-to-Point Protocol in a DSL Equal Access Deployment

This example describes the connection sequence for Point-to-Point Protocol (PPP) access to ISP services. For this example, SESM is deployed by a NAP providing equal access to several ISPs. The subscriber is a DSL subscriber using a PPP client configured on a laptop computer.

Note This example also uses the SESM captive portal features, explained in Chapter 4.

1. The subscriber launches the PPP client.
2. The PPP session is terminated on the Cisco router which is also the SSG platform.
3. System software on the router handles the PPP authentication. SSG receives notification when PPP authentication is successful. The SSG does not require further authentication.
4. The subscriber is authenticated but has no service connection. The SSG and SESM unconnected service redirection features can work together to provide the subscriber with a list of ISPs from which to choose.
   - The SSG unconnected service redirection feature intercepts the TCP packet containing the subscriber's first request. The request is redirected to an SESM application.
   - The SESM application retrieves the subscriber's profile and replies with a page containing the ISPs available to the subscriber, based on information in the profile.
   - The subscriber chooses an ISP. SESM requests the SSG to make the service connection.

Example Using Routed Wireless LAN

This example describes the connection sequence for routed access to SESM. For this example, the subscriber uses a PDA device configured for access through a wireless LAN access point.

1. The subscriber launches a web browser and sends an HTTP request. The TCP packet containing the request is routed through the SSG.
2. If the SSG TCP unauthenticated user redirect feature is configured, the subscriber can request any URL and the TCP packet is redirected to the SESM portal.
3. The SESM portal replies with the SESM logon page.
4. When the SESM portal receives the subscriber's logon information, the portal requests authentication services from the SSG. After the subscriber is authenticated, the SESM session is established.

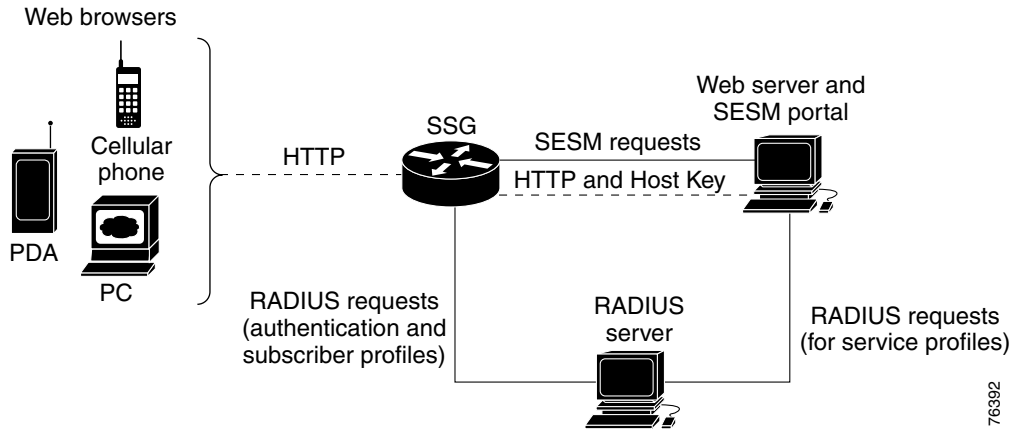
SESM RADIUS Mode Deployment

This section describes an SESM deployment using RADIUS mode. The section includes the following topics:

RADIUS Mode Deployment Diagram

Figure 3-2 shows a simplified view of SESM deployed in RADIUS mode and the communication mechanisms used between the various software components.

Figure 3-2 SESM Deployed in RADIUS Mode



SSG and the SESM portal work together to process subscriber requests. The processing sequence involves the following types of requests and associated replies:

- HTTP requests from the subscriber browser to the SESM portal—These requests are routed through the SSG to the SESM portal. If the port-bundle host key feature is enabled on the SSG, the SESM portal can support subscribers using overlapping and nonroutable IP addresses. See the "Subscriber Sessions" section on page 2-3 for more information.
- Requests from the SESM portal to SSG—SESM requests consist of proprietary command codes tunneled inside RADIUS requests.
- RADIUS protocol requests
  - From SSG to a RADIUS server—These are requests to authenticate the subscriber and obtain the subscriber profile.
  - From SESM to a RADIUS server—These are requests to obtain service profiles. The SESM portal caches the replies; therefore, these requests are required once for each service profile until the cache expires.

Request Processing in SESM RADIUS Mode Deployments

Table 3-1 describes the role of the SESM portal, SSG, and the RADIUS server in processing typical subscriber actions in RADIUS mode deployments. The mode determines where profile information is stored and obtained. Otherwise, the service selection and connection features work the same in RADIUS and SPE modes.

Table 3-1 Role of Components in SESM RADIUS Mode Deployments

Subscriber Action	Software Activity	Explanation
Subscriber logs on	Authenticate the subscriber in the system.	1. The HTTP request containing the logon information is routed to the SESM portal. 2. The SESM portal initiates authentication by sending an access request to the SSG. 3. SSG sends an access request to the RADIUS server. 4. The RADIUS server authenticates the subscriber and returns an access-accept or access-reject message to SSG. Access-accept messages contain the subscriber profile. 5. If the RADIUS reply is an access-accept, SSG creates an edge session on the router for the subscriber. 6. SSG replies to the SESM request in step 2. If the reply is an access-accept, it includes the subscriber profile originally obtained from the RADIUS server.
	Display web interface with: • Personalized content • List of subscribed services	7. The SESM portal can analyze the subscriber profile information and determine appropriate content for this subscriber. 8. The SESM portal ensures that it has a cached service profile for each of the services in the subscriber profile. If the cache is missing any of the profiles, the portal obtains the service profile from the RADIUS server. 9. The SESM portal replies to the HTTP request in step 1 with the appropriate content.

Table 3-1 Role of Components in SESM RADIUS Mode Deployments (continued)

Subscriber Action	Software Activity	Explanation
Subscriber selects a service	Access the service. Display updated service connection information.	1. The service connection request from the browser is routed to the SESM portal. 2. The SESM portal sends a connection request to SSG if the subscriber is authorized to connect to that service. 3. SSG does the following: – For passthrough services, it connects the service. – For proxy or tunnel services, it sends a RADIUS authentication request to a RADIUS server. If the reply is an access-accept, SSG connects the service. – SSG replies to the SESM request in step 2. To connect the service, SSG associates this subscriber's edge session with the service. When the connection is complete, SSG allows traffic from the subscriber to the domain specified in the service profile. 4. The SESM portal replies to the HTTP request in step 1 with updated service connection states.
Subscriber disconnects a service	Stop access to the service. Display updated service connection information.	1. The disconnection request from the browser is routed to the SESM portal. 2. The SESM portal sends a disconnect request to SSG. 3. SSG removes the association between the service and the subscriber's edge session and replies to the SESM request. 4. The SESM portal replies to the HTTP request in step 1 with updated service connection states.

RADIUS Mode Installation and Configuration Summary

Table 3-2 summarizes the steps required to deploy SESM in RADIUS mode.

Table 3-2 Configuration Requirements for SESM in RADIUS Mode

Deployment Step	References[1]
1. Install and configure a RADIUS AAA server.	• *Cisco Subscriber Edge Services Manager Deployment Guide* • Documentation from the RADIUS server vendor
2. Ensure that the SSG platform is running an appropriate Cisco IOS software release.	• *Release Notes for the Cisco Subscriber Edge Services Manager, Release 3.1(9)*

Table 3-2 Configuration Requirements for SESM in RADIUS Mode (continued)

Deployment Step	References[1]
3. Configure SSG. Use Cisco IOS commands on the SSG platform 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. – Configure SSG TCP redirect features (optional).	• *Cisco Subscriber Edge Services Manager Deployment Guide* • SSG documentation[2]
4. Install and configure the SESM portal application and J2EE-compliant web server.	• *Cisco Subscriber Edge Services Manager Installation Guide*
5. Create user and service profiles in the RADIUS database.	• *Cisco Subscriber Edge Services Manager Deployment Guide* • Documentation from the RADIUS server vendor

1. Go to http://www.cisco.com/univercd/cc/td/doc/solution/sesm/
2. Go to http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_4/122b4_sg/

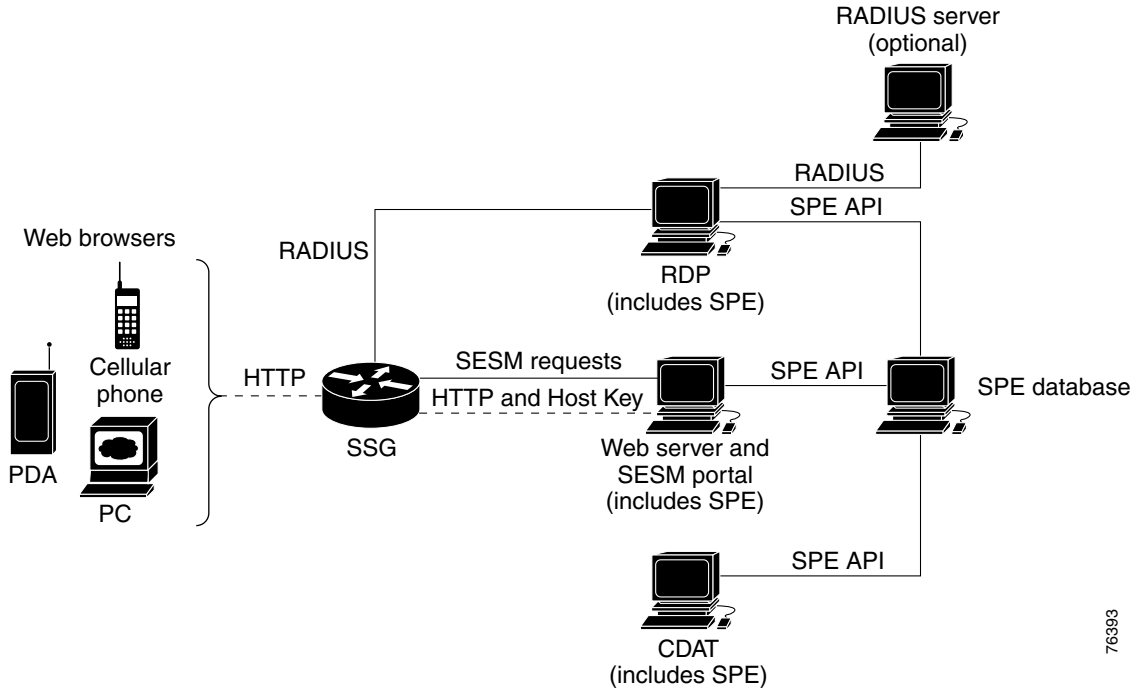
SESM SPE Mode Deployment

This section describes the service selection and connection solution using SESM deployed in SPE mode. The section includes the following topics:

SPE Mode Deployment Diagram

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

Figure 3-3 SESM Deployed in SPE Mode



In an SPE mode deployment, the Cisco Subscriber Policy Engine (SPE) provides services to SESM portals, CDAT, and RDP. The optional RADIUS server can provide user authentication services when RDP is configured in Proxy mode. SSG and SESM applications work together to process subscriber requests. The processing sequence involves the following types of requests and associated replies:

- HTTP requests from the subscriber browser to the SESM portal—These requests are routed through the SSG to the SESM portal. If the port-bundle host key feature is enabled on the SSG, the SESM portal can support subscribers using overlapping and nonroutable IP addresses. See the "Subscriber Sessions" section on page 2-3 for more information.
- Requests from the SESM portal to SSG—SESM requests consist of proprietary command codes tunneled inside RADIUS requests.
- RADIUS protocol requests from SSG to the RDP—These are requests to authenticate the subscriber and obtain the subscriber profile.

  When the RDP is running in Proxy mode, it forwards the RADIUS requests to a RADIUS server. Otherwise, RDP transforms the request into an LDAP request to the LDAP directory.
- LDAP protocol requests to the directory:
  - From RDP—These are requests for authentication and to obtain the subscriber profile.
  - From SESM—These are requests to obtain service profiles. The SESM portal caches the replies; therefore, these requests are required once for each service profile during an SESM portal run.
  - From CDAT

Request Processing in SESM SPE Mode Deployments

Table 3-3 describes the role of the SESM portal, RDP, SPE, and SSG in processing typical subscriber actions when the SESM portal is deployed in SPE mode. The mode determines where profile information is stored and obtained. Otherwise, the service selection and connection features work the same in RADIUS and SPE modes.

Table 3-3 Role of Components in an SPE Mode Deployment

Subscriber Action	Software Activity	Components Involved
Subscriber logs on	Authenticate the subscriber in the system.	**1.** The request from the browser containing the logon information is routed to the SESM portal. **2.** The SESM portal initiates authentication by sending an access request to the SSG. **3.** SSG sends a RADIUS protocol access request to the RDP. **4.** The RDP translates the request into an LDAP request to the LDAP directory. **Note** If the RDP is configured to run in Proxy Mode, RDP proxies the request to the configured RADIUS server. See the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*, Chapter 12 "Deploying SESM with SSG Solutions" for more information about the RDP Proxy mode. **5.** The LDAP directory replies to the RDP request. If access is granted (access-accept), the reply includes the subscriber profile. **6.** The RDP replies to the SSG request in step 3 with an access-accept or access-reject message. Access-accept messages contain the subscriber profile. **7.** If the reply is an access-accept message, SSG creates an edge session on the router for the subscriber. **8.** SSG replies to the SESM request in step 2. If the reply is an access-accept message, it includes the subscriber profile originally obtained from the directory in step 5.
	Display web interface with: • Personalized content • List of subscribed services	**9.** The SESM portal can analyze the subscriber profile information and determine appropriate content for this subscriber. **10.** The SESM portal ensures that it has a cached service profile for each of the services in the subscriber profile. If the cache is missing any of the profiles, the portal obtains the service profile from the LDAP directory. **11.** The SESM portal replies to the HTTP request in step 1 with the appropriate content.

Table 3-3 Role of Components in an SPE Mode Deployment (continued)

Subscriber Action	Software Activity	Components Involved
Subscriber selects a service	Access the service. Display updated service connection information.	1. The service connection request from the browser is routed to the SESM portal. 2. The SESM portal sends a connection request to SSG if the subscriber is authorized to connect to that service. 3. SSG does the following: – For passthrough services, it connects the service. – For proxy or tunnel services, it sends a RADIUS authorization request (to a RADIUS server or RDP). If the reply is an access-accept message, SSG connects the service. – SSG replies to the SESM request in step 2. To connect the service, SSG associates this subscriber's edge session with the service. When the connection is complete, SSG allows traffic from the subscriber to the domain specified in the service profile. 4. The SESM portal replies to the HTTP request in step 1 with updated service connection states.
Subscriber disconnects a service	Terminate access to the service. Display updated service connection information.	1. The disconnection request from the browser is routed to the SESM portal. 2. The SESM portal sends a disconnect request to SSG. 3. SSG removes the association between the service and the subscriber's edge session and replies to the SESM request. 4. The SESM portal replies to the HTTP request in step 1 with updated service connection states.
Subscriber updates an e-mail address	Update the LDAP directory.	The SESM portal sends the update to the directory using the SPE application programming interface.
Subscriber creates a subaccount	Update the LDAP directory.	The SESM portal sends the update to the directory using the SPE application programming interface.

SPE Mode Installation and Configuration Summary

Table 3-4 summarizes the installation and configuration activities for SESM in SPE mode.

Table 3-4 Configuration Requirements for SESM in SPE Mode

Activity	Reference[1]
1. (Optional) Install and configure a RADIUS server if you want to deploy RDP in Proxy mode and maintain separate profile sources for authentication (RADIUS) and authorization (LDAP).	• *Cisco Subscriber Edge Services Manager Deployment Guide* • Documentation from the RADIUS server vendor
2. Ensure that the SSG platform is running an appropriate Cisco IOS software release.	• *Release Notes for the Cisco Subscriber Edge Services Manager, Release 3.1(9)*
3. Configure SSG. Use Cisco IOS commands on the SSG platform 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. – Configure SSG TCP redirect features (optional).	• *Cisco Subscriber Edge Services Manager Deployment Guide* • SSG documentation[2]
4. Install and configure an SPE database.	• *Cisco Subscriber Edge Services Manager Deployment Guide* • Documentation from the directory vendor
5. Install and configure the SESM software components, which include: the SESM portal applications, a J2EE-compliant web server, RDP, SPE, and CDAT.	• *Cisco Subscriber Edge Services Manager Installation Guide*
6. Load sample data and create roles, groups, and user and service profiles in the LDAP directory.	• *Cisco Distributed Administration Tool Guide*

1. Go to http://www.cisco.com/univercd/cc/td/doc/solution/sesm/
2. Go to http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_4/122b4_sg/

SESM Service Selection Demo

This section describes some of the SESM features that you can demonstrate while running NWSP in Demo mode. Also see the "SESM Self-Care Demo" section on page 4-9 for demonstrations of account self-maintenance, subaccount creation, firewalls, and service self-subscription.

Step 1 Install NWSP in Demo mode. See the "Quick Start for Installing and Running Portals in Demo Mode" section on page A-2 for instructions.

Step 2 Start NWSP. The start script pathname is:

```
jetty
    bin
        startNWSP
```

See the "Starting a Demo" section on page A-5 for more information.

Step 3 Open a web browser and go to the NWSP page.

If the web browser is on the same system where NWSP is running, and you accepted the default port during installation, you can use the following URL:

```
http://localhost:8080
```

Otherwise, the URL is:

```
http://NWSPhostName:NWSPportNumber
```

Step 4 Log on using user IDs and passwords from Table 3-5. These values are the user IDs and passwords defined in the profiles in the installed demo data file for the NWSP application (demo.txt).

Table 3-5 Logon Names and Passwords in demo.txt

To demonstrate RADIUS Mode features...	To demonstrate SPE mode features...
User ID: radiususer Password: cisco	User ID: golduser Password: cisco
Other valid users for RADIUS mode demos are user1, user2, and so on, up to user45.	User ID: subgolduser Password: cisco **Note** subgolduser is a subaccount to golduser.

The NWSP home page appears. Figure 3-4 shows the home page for SPE mode. In RADIUS mode, the **MY ACCOUNT**, **MY SERVICES**, and **SUBACCOUNTS** tabs do not appear.

Figure 3-4 NWSP Home Page

The service selection list (the column on the left side of the window) shows all of the subscribed services for the logged-on user. The icons indicate:

- Green arrow—Connected service. In the radiususer and golduser profiles, the Internet service is marked as an automatically connected service; hence the green arrow icon indicating connection immediately after signing on.
- Red X—Unconnected service.

Step 5 Click on other services in the list to demonstrate service selection and connection. In particular, click on **Corporate Intranet** to show a service logon page for a service that requires authentication.

Because the profiles in data.txt do not include service names and passwords, you cannot demonstrate service logon. If you are demonstrating an LDAP deployment, click the **MY SERVICES** tab, and enter any username and password next to the service.

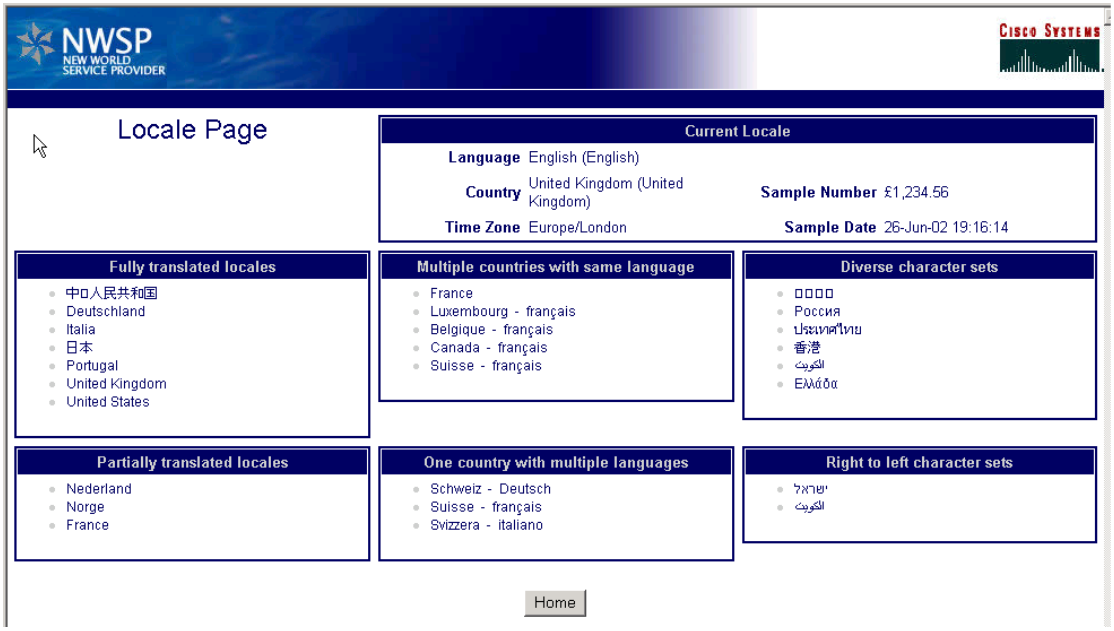
Step 6 Click the **STATUS** tab to show status information about services for the current SESM session. Figure 3-5 shows the NWSP status page.

Figure 3-5 NWSP Status Page

Step 7 Demonstrate service disconnection by clicking on the green arrow icon next to a connected service.

Step 8 Click the **SETTINGS** tab to show possibilities for localization and internationalization in the SESM portal. Figure 3-6 shows the NWSP Settings page.

Figure 3-6 NWSP Settings Page



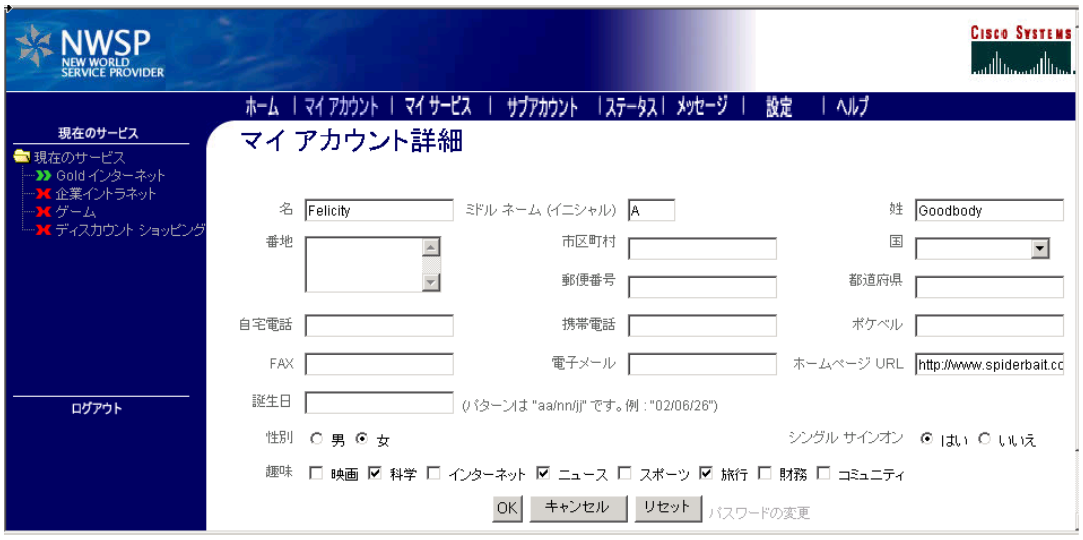
Step 9 To demonstrate translated resources:

1. From the Settings page, in the Fully translated locales box, click **Deutschland**.
2. Click the **HOME** button at the bottom of the window.
3. On the Home page, pass the cursor over the tabs to show tips in German.
4. Click the **STATUS** tab to show a status page containing German.

Step 10 To demonstrate text in resource bundles and images using the Japanese character set:

1. From the Settings page, in the Fully translated locales box, click the first bulleted item.
2. Click the **HOME** button at the bottom of the window.
3. Click any tab to show pages with Japanese resource bundles and images. Figure 3-7 shows the My Account page using the Japanese character set in the button and tab images and in translated resource bundles.

Figure 3-7 NWSP My Account Page Using Japanese Resources



If your browser does not display Japanese characters in text fields, download the Japanese font from one of the following web sites:

- For the Microsoft Internet Explorer browser, go to:

  http://www.microsoft.com/japan/

- For the Netscape browser, go to:

  http://wp.netscape.com/eng/intl/

Note For UTF-8 support, use Netscape Version 6 or later.

Step 11 To return to the Settings page, click the tab that is second from the right.

Step 12 To end the current session:

1. Click the **HOME** button.

2. Click the **LOG OUT** button.