CHAPTER 3

Feature Descriptions

This chapter describes the features in the Cisco Subscriber Edge Services Manager (SESM). The topics in this chapter are:

Web Portal for Subscribers

This section describes the key features that are visible to subscribers who access an SESM web portal.

Subscriber Features

An SESM web portal provides the web interface from which subscribers can:

- Authenticate—The SESM portal provides a logon window for subscribers.
- Select one or more services for connection—The SESM portal presents a list of subscribed services based on the subscriber profile. The subscriber connects to services by selecting them from the list. If appropriate, SESM can display a service logon page.
- Disconnect from services—Subscribers can disconnect from a single service, or by logging off of SESM, disconnect from all services.
- View session status information—Subscribers can see which services are active in their current session and view other session status information.

When SESM is deployed in LDAP mode, the following additional capabilities can be offered to subscribers:

- Change account information
- Self-subscribe to services
- Create subaccounts on a main account

Customized and Branded Web Portal

A web designer can customize the look and feel of the SESM web portal to conform to the brand identity required by the deployer. Customization includes the ability to have a different appearance for separate user groups, locations, access devices, services, and other subscriber connection attributes.

Personalized Subscriber Experiences

An SESM web portal can be personalized such that each subscriber sees pages appropriate to his or her usage, access type, and preferences. Some of the features that provide for a personalized subscriber experience are:

- Subscribed Services—The service selection feature presents a personalized list of subscribed services for each subscriber. This information is obtained from the subscriber profile.
- Device, Locale, and Brand awareness—The awareness features choose the appropriate resources to use in shaping the pages that are returned to the subscriber's browser.
- Self-management features—The self-management features available in LDAP mode allow the subscriber to control account information.
- Advertisements—The captive portal feature can deliver advertisement content that is directed at subscriber interests identified in the profile (LDAP mode only) or based on currently subscribed services.
- Personal options—Some options within a subscriber profile offer further personalization. For example, you can specify a home URL for Internet connections. Another option allows automatic connections to specified services on a per subscriber basis.

Authentication Options

Subscribers must authenticate by logging on to the SESM portal before they can select and connect to services. (The exception is open garden services that might be configured on the SSG.)

SESM passes the credentials to the SSG in a RADIUS protocol format. A RADIUS server performs the verification procedures. In LDAP mode, the RADIUS server is the SESM RDP server. The RADIUS server verifies against attribute values stored in the subscriber profile.

SESM supports the following authentication schemes:.

- 2-Key Authentication, page 3-3
- 3-Key Authentication, page 3-3
- Single Sign-on for PPP Clients, page 3-4
- Single Sign-on for non-PPP Clients, page 3-4

2-Key Authentication

The 2-key authentication method bases authentication against the following attributes stored in the subscriber profile:

- User name
- Password

The sample SESM portal applications display a logon page that prompts for the two values listed above. SESM passes these values to SSG as standard RADIUS protocol attributes.

3-Key Authentication

Deployments in wireless environments might require authentication based on attributes in addition to user name and password. For example, authentication could be based on the following attributes:

- User name
- Password
- A third attribute, such as:
  - Access point name (APN)—This is RADIUS attribute 30, CALLED_STATION_ID. This might be a GGSN.
  - MSISDN—This is RADIUS attribute 31, CALLING_STATION_ID. This might be the subscriber's MSISDN or telephone number.
  - Subscriber's telephone number—SESM supports authentication against a telephone number by putting the phone number in the RADIUS attribute 31, CALLING_STATION_ID field.
  - Network access server (NAS) identifier—This is attribute 32, NAS_IDENTIFIER. In SESM deployments, the SSG is the NAS.

A web developer can customize an SESM web portal to use a logon page that prompts for telephone number in addition to user name and password. A sample 3-key logon page is included in the SESM web developer kit. See the *Cisco Subscriber Edge Services Manager Web Developer Guide* for more information. SESM passes the telephone number to SSG as standard RADIUS attribute 31, CALLING_STATION_ID. If no value is supplied on the login page, SESM inserts the user name in this field.

The SESM web developer kit does not offer a way to collect an APN or NAS identifier and send it to SSG. SSG includes this support. See the SSG documentation for details.

To implement 3-key authentication:

- If SESM is deployed in RADIUS mode, business logic to verify against three keys must exist in the RADIUS server you are using. See the RADIUS server vendor.
- If SESM is deployed in LDAP mode, you can configure the RDP Server to perform 3-key authentication using any number and any combination of standard RADIUS attributes.

In an LDAP directory, administrators can enter the APN and NAS identifier attributes as group values. See the *Cisco Distributed Administration Tool Guide* for more information.

Single Sign-on for PPP Clients

The single sign-on feature removes the requirement for point-to-point protocol (PPP) clients to enter authentication details twice. When single sign-on is enabled, the SESM portal does not ask a PPP subscriber to authenticate (log on). Instead, the SESM portal uses the PPP authenticated identity from SSG.

Single Sign-on for non-PPP Clients

The single sign-on feature also has meaning for non-PPP subscribers. With single sign-on, if any subscriber authenticates using the SESM web portal, that subscriber does not need to sign on again for the duration of the session. The session exists as long as SSG still has a host object for it. This feature has advantages for subscribers in the following situations:

- The subscriber can stop the browser or navigate away from the SESM portal pages, and then return to the SESM pages later and not be required to reauthenticate.
- The subscriber does not need to reauthenticate if SESM automatic memory management clears sessions from the SESM portal.

Service Selection and Connection

The SESM portal application presents a service list from which the subscriber can select one or more services for connection. The connection features are implemented by SSG and controlled by attributes stored in the subscriber or service profiles.

Service Selection

After a subscriber authenticates, the SESM portal application displays subscribed services obtained from the subscriber profile. From the list of displayed services, the subscriber selects one or more services for connection. The portal can also display service groups, as defined in service group profiles. The web developer controls the format of the service list and how to portray service groups.

Service Authentication and Authorization

A preliminary level of service authorization is implied by the service selection list presented to a subscriber. The SESM portal presents for selection only those services to which a subscriber is subscribed, according to the subscriber profile. In LDAP mode, when a subscriber self-subscribes to a new service, that service is added to the subscriber profile and immediate access to that service is possible.

The SESM web portal can present a service authentication page for services that require it. Service authentication can be based on user name and password. For proxy services, an option in the service profile specifies whether the CHAP or PAP protocol is used to authenticate for the service.

Automatic Connections

With automatic connection, the subscriber gains access to a service immediately after authenticating, without manually selecting the service from the SESM portal. Depending on configuration options, either SSG or SESM performs the connection immediately after the subscriber authenticates.

A service is marked as an autoconnect service in the subscriber profile. By default, an autoconnect service is hidden from the service list on the service selection page, but another option in the subscriber profile can specify that it be included in the list. In LDAP mode, the SESM portal application can offer the subscriber the means to self-select or change the services that should be automatically connected.

Providers can use the automatic connection option as a way to provide always-on services or as a way to bypass the service selection feature. For example, a provider might choose to offer three always-on services to all subscribers, and mark those services as autoconnected in all subscriber profiles. If these are the only services offered by the provider, and the profiles indicate that they are hidden from the service selection list, the web portal could be customized to omit the service selection page.

Service Status

Information about services that were connected during the current session can be displayed in an SESM web portal. The web developer controls the types of information that are displayed on the status page and how it is presented. See the *Subscriber Edge Services Manager Web Developer Guide* for more information.

You can see a sample status page in the NWSP application. The sample page shows the following information about all connected services (including automatically connected services) during the current session:

- Currently connected services
- Services that were connected during the session but are currently not connected
- Connection length of time (for both current and previously connected services)
- Transmitted and received byte count on a per service basis

The SESM web developer kit provides a way to link images to a service status for display on the portal pages. For example, the NWSP uses the following images:

- No light—Indicates that the service is not selected for connection
- Red light—Indicates an unconnected service
- Green light—Indicates a connected service

Mutually Exclusive Service Selection

Mutually exclusive service selection restricts a subscriber to accessing only one service at a time in a specified group of services. One use of this feature is described in the "Service Selection by Bandwidth" section on page 3-6.

A service group is a collection of services defined in a service group profile. A subscription to a service group implies subscription to all of the services in the group. It also implies the ability to select all of the services in the group. When a group is defined as mutually exclusive, SESM limits service selection to one service at a time within the group.

An SESM configuration option controls the SESM action when a subscriber is already logged into one service and then selects another service in the group:

- SESM can automatically request SSG to disconnect the first service and connect the new service.
- SESM can prompt the subscriber to log off the first service. After the subscriber logs off, SESM requests the connection to the other service.

Note SESM waits for the first service to be disconnected before requesting connection to the new service. If the connection to the new service fails, the subscriber is not connected to either service.

A mutually exclusive service group is defined in a service group profile. For RADIUS mode deployments, see Appendix D, "Configuring RADIUS," for more information. For LDAP mode deployments, see the *Cisco Distributed Administration Tool Guide*.

Service Selection by Bandwidth

An SESM web portal can support the SSG hierarchical policing feature in Cisco IOS Release 12.2(4)B by allowing subscribers to choose a different bandwidth from their regularly subscribed bandwidth for a particular service. For example, a subscriber might be subscribed to an Internet or video service with a 128-Kbps bandwidth, but have the option to select 512 Kbps or 1 Mbps service on demand.

To implement this feature, define the bandwidth options for each service as separate and mutually exclusive services within a service group. This restriction is important to prevent subscribers from simultaneously connecting to (and being billed for) the same service over two different bandwidths.

Supported Service Types

The service type is one of the attributes in a service profile. Service type is known as service class in service profiles on an LDAP directory.

SESM can support a wide range of service types. In general, SESM supports the service types that are supported by the other elements in the network, such as the SSG.

In Cisco IOS Release 12.2(4)B, the SSG supports the following types of service:

- Passthrough—The SSG can forward traffic through any interface using normal routing or a next-hop table. Passthrough service is ideal for standard Internet access.
- Proxy—When a subscriber selects a proxy service, the SESM portal prompts for another user name and password. After authentication, the service is accessible until the user logs out from the service, logs out from the SESM portal, or is timed out.
- Tunnel—When a subscriber selects a tunnel service, SESM determines if the SSG single host logon feature is configured and if the subscription has the credentials for the service connection. If both conditions are true, SESM sends a connection request. Otherwise, SESM displays an authentication page to obtain service connection credentials from the subscriber.

Features in SESM-SPE

These features are implemented by the SPE component and are therefore available only when SESM is deployed in LDAP mode. To implement these features, you must install and configure SESM in LDAP mode, and populate the LDAP directory with valid subscriber information.

For more information about these features, see the following:

- The *Cisco Distributed Administration Tool Guide* describes how to provision a subscriber with the appropriate permission to perform these tasks.
- The *Cisco Subscriber Edge Services Manager Web Developer Guide* describes how to implement these features in an SESM web portal.

Subscriber Account Self-Management

Subscriber account self management allows subscribers to change their own account details, such as address information, phone numbers, passwords for account authentication, and credentials for proxy and tunnel service authentications. (Passwords are encrypted.) This subscriber updating capability relieves the service provider from time-consuming maintenance tasks.

Subscriber Service Self-Subscription

Self-subscription allows subscribers to sign up for 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.

Subscriber Subaccount Creation and Management

Subscriber subaccount creation and management 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, and control whether the subaccounts can subscribe to services themselves.

The service provider can impose limits on the number of subaccounts in a main account. This feature allows providers to sell accounts of differing sizes. It also prevents pranksters from creating an endless number of subaccounts.

Extended Subscriber Profile Data

SESM in LDAP mode supports many of the fields in the X.500 standard user schema developed for use with LDAP. Some of the fields supported include date of birth, various address and telephone number fields, e-mail, gender, and hobbies. These additional user data fields can optionally be included in a subscriber profile. The information can be maintained by the deployer using CDAT or by the subscriber using the self-management features in the SESM portal.

Role Based Access Control

Role based access control (RBAC) is an access model that defines access privileges for roles, rather than for individuals, and then assigns individuals to a role. The Cisco implementation extends the model, allowing administrators to manage groups of subscribers, rather than individuals. Using this group-based 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 RBAC model applies to data stored in an LDAP directory using the SPE extensions that are delivered as part of the SESM LDAP mode installation. Administrators use the Cisco Distributed Administration Tool (CDAT) to enter and manage the RBAC data in the directory.

See the *Cisco Distributed Administration Tool Guide* for more information about RBAC.

Captive Portal Features

The SESM captive portal solution works with the TCP redirect features on the SSG to provide several types of subscriber captivation. With captivation, a subscriber's request is captured and handled in an appropriate manner.

The SSG TCP redirect feature redirects incoming TCP packets to a specified SESM captive portal application. The captive portal application issues an HTTP redirection to the subscriber's browser, directing it to another application that returns content to the subscriber. These content applications can be SESM web portals that enforce account authentication and service authorizations or present advertising and message pages.

The following sections briefly describe the types of TCP redirection and captivation supported by the SSG in Cisco IOS Release 12.2(4)B and SESM Release 3.1(3). For more information about captive portal features, configuration details, and corresponding SSG TCP redirect requirements, see Chapter 8, "Deploying a Captive Portal Solution."

Unauthenticated User Captivation

Unauthenticated subscribers are those who have submitted an HTTP request when there is no host object on the SSG. A host object exists only after successful authentication. This situation occurs when the subscriber opens a browser and issues a request (or has a home page setting) to a location other than an SESM logon page. Unauthenticated subscriber captivation in a wireless LAN allows unauthenticated access to the LAN but then requires the subscriber to authenticate before accessing the Internet or other services.

The SSG TCP redirect feature redirects unauthenticated packets to the captive portal application. The SESM captive portal solution can redirect the browser to the login page of an SESM web portal. The captive portal solution can also preserve the originally requested service location and redirect again to connect the subscriber to it.

One effect of deploying unauthenticated subscriber redirections is that subscribers do not need to know the URL to the SESM logon page because they are sent there automatically when they start a browser session. Also, after authenticating, they can be redirected to a home page URL or a service address.

Unconnected Service Captivation

Service redirection handles requests to service domains to which the subscriber has not yet connected. Rather than rejecting these requests, the SSG TCP redirect feature can redirect them to an SESM captive portal application, which can then handle the request in an appropriate way to gain connection or present some explanation to the subscriber.

Some examples of how an SESM captive portal solution can support service captivations are:

- When a subscriber is not authenticated for a service, the captive portal solution can present a service logon page or perform the authentication on behalf of the subscriber.
- When the subscriber is not subscribed to a service, the captive portal solution can present a subscription page.
- When service connection is refused because of lack of funds, the captive portal solution can present an explanation. See the "Prepaid Services" section on page 3-13 for more information.

Initial Logon Captivation

Initial logon captivation presents all subscribers with a message or greetings page. The TCP redirect feature redirects all authenticated subscribers to the captive portal application. The captive portal solution can present any type of message for a specified length of time, after which the browser is redirected again to the originally requested service, or to an SESM service selection page, or to an automatically connected service.

Advertisement Captivation

Advertisement captivation presents advertisements at specified intervals for specified durations. The TCP redirect feature handles the interval timer and redirects the next TCP packet originating from the subscriber to the captive portal application The captive portal solution presents the advertisement content. The captive portal solution can also present service-specific advertisements by identifying the service name or service URL that is being requested, and presenting advertisements appropriate to users of the service.

Enhanced Session Management with Port-Bundle Host Key

The port-bundle host key feature on the SSG ensures that each currently logged-on subscriber is uniquely identified, regardless of the IP address being used. This is an optional feature, but when enabled, it allows SESM portals 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 can support subscribers at sites using private IP addressing schemes, including subscribers of ISPs using private addressing schemes.

The SSG port-bundle host key feature also enhances configuration of large SESM deployments. With port-bundle host key, you do not need to map client subnets to SSGs.

Location Awareness

An SESM portal can derive the location of the subscriber and present different retail pages or different elements within a page based on location. SESM offers several ways to determine location.

Location Awareness Based on Configuration

In the portal MBean configuration file, you can add entries that associate a location with known configuration attributes, such as:

- SSG IP address—This method assumes that all requests to a particular range of SSG IP addresses are located in the same area.
- Client subnet—This method assumes that all requests from a particular range of client addresses are located in the same area.

Note The port-bundle host key feature obscures the client subnet. When the SSGs are configured to use port-bundle host key, infer location from the SSG IP address rather than the client subnet.

Location Awareness Based on Attributes in the HTTP Request

You can customize an SESM portal to derive the location from attributes in the subscriber’s original HTTP request. The SESM web development kit includes a location attribute.

Brand Awareness

An SESM portal can derive the brand of the subscriber and present different retail pages or different elements within a page based on brand. SESM offers several ways to determine brand.

Brand Awareness Based on Subscriber Groups

You can use subscriber groups to represent brands. The group is an attribute of a subscriber profile. The SESM portal detects the branding for a subscriber based on the group in which that subscriber is assigned and returns pages appropriate to the brand of that group.

Note Subscriber groups are known as user groups in CDAT and the RADIUS profiles.

An SESM portal can implement differences among branded groups in many ways, including:

- Each brand could have different subscriber privileges.
- Each brand could have different subscribed and available services.
- Each brand could have different looks to the browser pages, such as different colors or different menu options.

The sample data installed with SESM defines three subscriber groups for branding purposes: bronze, silver, and gold groups. The sample data also defines one user for each of these groups: bronzeuser, silveruser, and golduser. To illustrate branding possibilities, PDA uses a different look and different colors for each brand. NWSP uses different menu options.

Brand Awareness Based on Configuration

You can add entries to the portal’s MBean configuration file that associate a brand with the SSG IP address or client subnet, as described in the “Location Awareness Based on Configuration” section above.

Web Development Features

The SESM web development kit includes technologies and development features for customizing an SESM web portal. See the *Cisco Subscriber Edge Services Manager Web Developer Guide* for detailed descriptions of the following and additional web development features.

Localization and Internationalization

Web developers can use the following techniques to localize and internationalize an SESM web portal.

- An SESM web portal can use conventional Java techniques for internationalization and localization.
- SESM includes additional development components that improve upon the standard Java locale-related classes and help reduce the complexity of localizing an SESM web application. Some localization subjects addressed by the SESM components are: time zone, language, and preferred formats for currency, numbers, dates, and times.
- Resource bundles contain locale-specific data that varies depending on the user's language and region, such as translatable text for status and error messages and for labels on GUI elements. The developer can add additional resource bundles to a web application to accommodate new locales.

Java Server Pages

JSPs provide a standard way to integrate Java code with HTML, XML, and WML. The SESM portal and captive portal applications use JSPs to present interactive, dynamically updated, personalized, and branded web pages to subscribers.

The JSP pages contain the elements that the developer modifies for the specific requirements of the provider. No servlet programming is required.

SESM User Shape Mechanism

The SESM user shape mechanism is a method for combining any number of subscriber attributes to determine which resources to use in the JSP returned to a subscriber. This mechanism eases the task of adding more attributes to the decision.

Locale and Device Awareness

The SESM portal detects information about a subscriber from the header of the initial HTTP request. For example:

- The subscriber's preferred language setting in the browser sets the locale.
- Information about the access device, browser type, and the connection location is available from the header.

The portal developer can use one or all of these attributes in the user shape to determine the look and feel of the JSP returned to the subscriber's browser. For example:

- If the subscriber's browser language is French and the receiving device is a desktop PC, the response can be rendered in French using HTML.
- If another subscriber's browser language is Spanish and the receiving device is a WAP cell phone, the response can be rendered in Spanish using Wireless Markup Language (WML).

Library Resources

The SESM development components include Dreamweaver templates and library items.

Dreamweaver templates can be very useful for customizing or maintaining a web application's JSP pages when many pages have the same layout. By modifying a template and then updating the JSP pages that use the template, you can change the look and feel of an entire set of pages very quickly.

Dreamweaver library items contain Body elements such as images, text, and other objects that are reused throughout the JSP pages. Each sample SESM web application includes a complete set of customizable images, buttons, and a navigation bar.

Scaling, Redundancy, and Resiliency Features

An SESM web portal offers the following scaling, redundancy, and resiliency features:

- You can deploy multiple instances of the same SESM web portal and balance the load as you would with any web server application. The Cisco Content Services Switch 11000 is recommended for load balancing.
- The SSG port-bundle host key feature simplifies large deployments because it eliminates manual mapping of subscriber subnets to SSGs.
- SESM applications are highly resilient because they are completely stateless regarding subscriber sessions. SESM applications obtain session status information from the SSG. Therefore, the SESM applications can be started and stopped without affecting a subscriber.

For more information about scaling and redundancy in an SESM deployment, see the following:

- Vendor documentation for the load balancing tool.
- The "Memory Requirements and CPU Utilization" section on page 7-8 shows memory usage requirements for an SESM web portal application.
- *SSG Features in Release 12.2(4)B* describes how to configure the port-bundle host key feature on the SSG.

Accounting and Billing Interfaces

The accounting and billing solutions that work with an SSG/SESM deployment are based on actual services used and the duration of use. These interfaces are implemented and configured on the SSG.

RADIUS Accounting

SSG can be configured to send accounting requests to a RADIUS server. The RADIUS server generates the accounting records. See the "Configuring the RADIUS Accounting Feature" section on page D-11 for a summary of how to configure this solution.

Prepaid Services

The SSG Prepaid feature in Cisco IOS Release 12.2(4)B and later supports an interface to a third-party billing server. The third-party server performs billing and accounting functions, which can include prepaid services features. See *SSG Features in Release 12.2(4)B* for more information about the SSG Prepaid feature.

Enhancing Prepaid Services Using SESM Captive Portal

The SESM captive portal features can be used in conjunction with the SSG prepaid feature to enhance the subscriber's experience in a prepaid business model. When service connection is refused or a current session is disconnected because of lack of funds, the SESM captive portal solution can display a message page to the subscriber explaining the reasons for the service refusal.

In a prepaid services business model, service connection is denied (unauthorized) if there are no funds in the subscriber's account. The SSG Prepaid feature allows SSG to check a subscriber's available credit to determine whether to connect the subscriber to a service and how long the connection can last. The SSG Prepaid feature also supports reauthorizations after connection is granted. If funds are depleted for the account, SSG logs the subscriber off the service.