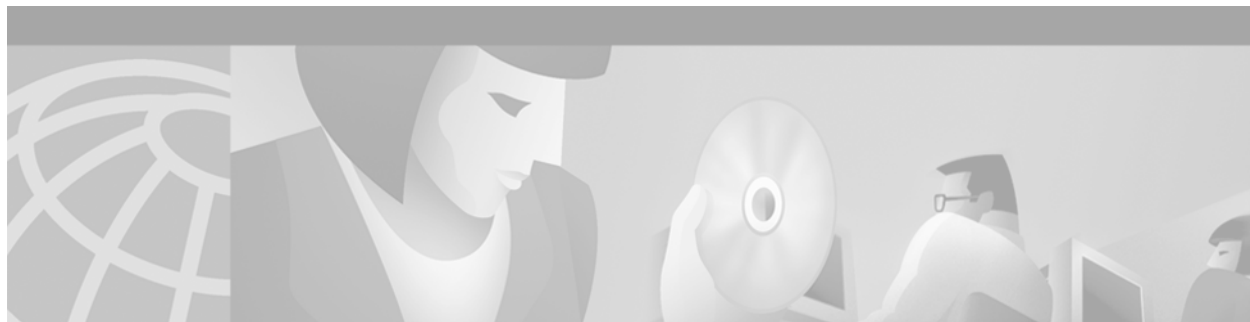




SSG Prepaid

Feature History

Release	Modification
12.2(4)B	This feature was introduced.

This document describes the SSG Prepaid Billing feature in Cisco IOS Release 12.2(4)B. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 6](#)
- [Supported Standards, MIBs, and RFCs, page 6](#)
- [Prerequisites, page 7](#)
- [Configuration Tasks, page 7](#)
- [Configuration Examples, page 8](#)
- [Command Reference, page 8](#)
- [Glossary, page 12](#)

Feature Overview

The SSG Prepaid feature expands Service Selection Gateway (SSG) accounting features to allow service providers to offer prepaid billing for their services.

SSG

SSG is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as digital subscriber lines, cable modems, or wireless to allow simultaneous access to network services.

SSG works in conjunction with the Cisco Service Selection Dashboard (SSD) or its successor product, the Cisco Subscriber Edge Services Manager (SESM). Together with the SESM or SSD, SSG provides subscriber authentication, service selection, and service connection capabilities to subscribers of Internet services. Subscribers interact with an SESM or SSD web application using a standard Internet browser.

SSG acts as a central control point for Layer 2 and Layer 3 services. These can include services available through ATM virtual circuits (VCs), virtual private dial-up networks (VPDNs), or normal routing methods.

SSG communicates with the authentication, authorization, and accounting (AAA) management network where RADIUS, Dynamic Host Configuration Protocol (DHCP), and Simple Network Management Protocol (SNMP) servers reside and with the Internet service provider (ISP) network, which may connect to the Internet, corporate networks, and value-added services.

A licensed version of SSG works with the SESM or the SSD to present to subscribers a menu of network services that can be selected from a single graphical user interface (GUI). This functionality improves flexibility and convenience for subscribers and enables service providers to bill subscribers for connect time and services used, rather than charging a flat rate.

For more information about SSG, refer to the *Service Selection Gateway* feature module in the “New SSG Features in Release 12.2(4)B” area of Cisco.com.

How SSG Prepaid Works

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 subscriber's credit is administered by the billing server as a series of quotas representing either a duration of use (in seconds) or an allowable data volume (in bytes). A quota is an allotment of available credit.

To obtain the first quota for a connection, SSG submits an authorization request to the AAA server. The AAA server contacts the prepaid billing server, which forwards the quota values to SSG. SSG then monitors the connection to track the quota usage. When the quota runs out, SSG performs reauthorization. During reauthorization, the billing server may provide SSG with an additional quota if there is available credit. If no further quota is provided, SSG logs the user off.

The following sections describe in more detail how authorization and reauthorization work:

- [Service Authorization, page 2](#)
- [Service Reauthorization, page 4](#)

Service Authorization

SSG differentiates prepaid services from postpaid services by the presence of the Service Authorization vendor-specific attribute (VSA) in the service profile. The presence of this attribute in the service profile means that SSG must perform authorization before providing access to the service. [Table 1](#) describes the Service Authorization VSA.

Table 1 Service Authorization VSA Description

Attribute ID	Vendor ID	Subattribute ID and Type	Attribute Name	Subattribute Data
26	9	251 Service-Info	Service Authorization	The value “Z” indicates that authorization is required.

Once a service has been identified as prepaid, SSG generates an Access-Request called a Service Authorization Request. The content of this new type of Access-Request is described in [Table 2](#).

Table 2 **Content of Service Authorization Request**

Attribute Number	Attribute Name	Description	Notes
1	User-Name	MS Subscriber Name	
2	PAP Password	Global Service Profile Password	
4	NAS IP Address	SSG IP Address	
6	Service-Type	Framed-User	
26	Vendor-Specific	Name of Service	Subattribute ID 251; code N.
31	Calling-Station-ID	MSISDN	The User-Name may appear in this field if the access technology does not provide an MSISDN.
55	Time-Stamp	Time-Stamp	
44	Acct-Session-ID	Session ID	
61	NAS-Port-Type	Async (value=o)	

The prepaid billing server performs authorization based on the same key that was used for authentication. For example, in a mobile wireless scenario where the unique key that is used for authentication is the Calling-Station-ID attribute (attribute 31), the quota authorization would also be performed based on the Calling-Station-ID attribute.

The AAA server responds to the Service Authorization Access-Request with an Access-Accept that defines the quota parameters for the connection. The Access-Accept for a Service Authorization Request is described in [Table 3](#). Authorization for a service is provided based on the presence and content of the Quota VSA in the Access-Accept.

Table 3 **Content of Service Authorization Access-Accept**

Attribute Number	Attribute Name	Description	Notes
6	Service-Type	Framed-User	
26	Vendor-Specific	Quota	Subattribute ID: 253. The value “Q” indicates that this is the Quota VSA.

[Table 4](#) describes the new Quota VSA.

Table 4 **Quota VSA**

Attribute ID	Vendor ID	Subattribute ID and Type	Attribute Name	Subattribute Data
26	9	253 Control-Info	Quota	Q—Control-Info code for prepaid quota. T or V—Quota subcode for time or volume. numeric string—Quota value.

If a nonzero quota is returned, SSG creates a connection to the service with the initial quota value in seconds for time and bytes for volume. A value of zero in a quota means the user has insufficient credit and is not authorized to use that service, and the connection is not made. If the Quota attribute is not present in the authorization response, SSG treats the connection as postpaid.

Service Reauthorization

During the connection, SSG decrements a volume-based quota until it runs out. If the quota is based on time, the connection is allowed to proceed for the quota duration. When the quota reaches zero, SSG issues a Service Reauthorization Request to the billing server. The Service Reauthorization Request includes a new SSG VSA called Quota Used. The Quota Used VSA has the same format as the Quota VSA described in [Table 4](#). The Service Reauthorization Request is defined in [Table 5](#).

Table 5 **Content of Service Reauthorization Request**

Attribute Number	Attribute Name	Description	Notes
1	User-Name	MS Subscriber Name	
2	PAP Password	Global Service Profile Password	
4	NAS IP Address	SSG IP Address	
6	Service-Type	Framed-User	
26	Vendor-Specific	Name of Service	Subattribute ID 251; code N.
26	Vendor-Specific	Quota Used	Subattribute ID 253. The Quota Used VSA has the same format as the Quota VSA.
31	Calling-Station-ID	MSISDN	
55	Time-Stamp	Time-Stamp	
44	Acct-Session-ID	Session ID	
61	NAS-Port-Type	Async (value=o)	

If service reauthorization is unsuccessful, the billing server will respond to the Service Reauthorization Request with an Access-Accept containing a quota of zero. SSG will terminate the connection to the service at this point. If service reauthorization is successful, the billing server will return another quota to SSG and the connection will be allowed to continue.

Benefits

Real-Time Billing

The SSG Prepaid feature allows for real-time billing with maximum flexibility, regardless of the type of service and billing scheme. Users can be billed on a flat rate, air-time, or volume basis.

Concurrent Service Access

The SSG prepaid solution is capable of supporting concurrent service access. SSG services can be configured for concurrent or sequential access. Concurrent access allows users to log on to a service while simultaneously connected to other services. Sequential access requires that the user log off from all other services before accessing a service.

Restrictions

- Quotas are measured in seconds for time or bytes for volume. There is no way to change the unit of measure.
- The volume quota is for combined upstream and downstream traffic.
- SSG does not support simultaneous time and volume quotas for the same service connection.

Related Features and Technologies

- Mobile wireless
- RADIUS
- Service Selection Gateway (SSG)

Related Documents

For more information about SSG, refer to the following document:

- *Service Selection Gateway*, Cisco IOS Release 12.2(4)B feature module

For information about other supported SSG features, refer to the following documents:

- *Hierarchical Policing for Service Selection Gateway*, Cisco IOS Release 12.2(4)B feature module
- *SSG Autodomain*, Cisco IOS Release 12.2(4)B feature module
- *SSG AutoLogin Using Proxy Radius*, Cisco IOS Release 12.2(4)B feature module
- *SSG Autologoff*, Cisco IOS Release 12.2(4)B feature module
- *Service Selection Gateway Accounting Update Interval per Service*, Cisco IOS Release 12.2(4)B feature module
- *SSG Open Garden*, Cisco IOS Release 12.2(4)B feature module

- *SSG Port-Bundle Host Key*, Cisco IOS Release 12.2(4)B feature module
- *SSG TCP Redirect for Services*, Cisco IOS Release 12.2(4)B feature module

For information on configuring SSD and SESM, refer to the following documents:

- *Cisco Subscriber Edge Services Manager and Subscriber Policy Engine Installation and Configuration Guide*
- *Cisco Service Selection Dashboard Installation and Configuration Guide*
- *Cisco Service Selection Dashboard Web Developer Guide*

For more information about configuring RADIUS, refer to the following documents:

- The chapter “Configuring RADIUS” in the *Cisco IOS Security Configuration Guide*, Release 12.2
- The chapter “RADIUS Commands” in the *Cisco IOS Security Command Reference*, Release 12.2

Supported Platforms

- Cisco 6400 series
- Cisco 7200 series
- Cisco 7401 ASR

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

- SSG accounting must be enabled in order for the SSG Prepaid feature to be used. SSG accounting is enabled by default. If it has been disabled, reenable it by using the **ssg accounting** command in global configuration mode.
- The SSG Prepaid feature requires the AAA server to have prepaid billing support.

Configuration Tasks

See the following sections for configuration tasks for the SSG Prepaid feature. Each task in the list is identified as either required or optional.

- [Configuring SSG Prepaid](#) (required)
- [Verifying SSG Prepaid](#) (optional)

Configuring SSG Prepaid

To configure SSG to provide the prepaid billing server with session ID and time-stamp information, use the following commands in global configuration mode:

Command	Purpose
Router(config)# radius-server attribute 44 include-in-access-req	Sends RADIUS attribute 44 (Accounting Session ID) in access request packets before performing user authentication (including requests for preauthentication).
Router(config)# radius-server attribute 55 include-in-acct-req	Sends RADIUS attribute 55 (Event-Timestamp) in accounting packets.

Verifying SSG Prepaid

To verify the configuration of the SSG Prepaid feature, use one or both of the following commands in EXEC mode:

Command	Purpose
Router# show ssg connection <i>ip-address service-name [interface]</i>	Displays information about the host's connection to the specified service, including quota information for prepaid connections.
Router# show running-config	Displays the contents of the currently running configuration file.

Monitoring and Maintaining SSG Prepaid

To monitor and maintain SSG prepaid functionality, use the following commands in privileged EXEC mode:

Command	Purpose
Router# debug radius	Displays information associated with RADIUS.
Router# debug ssg ctrl-events	Displays all event messages for control modules.
Router# debug ssg ctrl-packets	Displays packet contents handled by control modules.
Router# debug ssg data	Displays all data path packets.

Configuration Examples

This section provides the following configuration example:

- [SSG Prepaid Configuration Example](#)

SSG Prepaid Configuration Example

The following example shows how to configure RADIUS attributes 44 and 55 to support SSG prepaid billing services:

```
radius-server attribute 44 include-in-access-req
radius-server attribute 55 include-in-acct-req
```

Command Reference

This section documents modified commands. All other commands used with this feature are documented in the *Service Selection Gateway* feature module for Cisco IOS Release 12.2(4)B or the Cisco IOS Release 12.2 command reference publications.

- [show ssg connection](#)

show ssg connection

To display the connections of a given host and a service name, use the **show ssg connection** command in privileged EXEC mode.

show ssg connection *ip-address service-name [interface]*

Syntax Description	<i>ip-address</i>	IP address of an active SSG connection. This is always a subscribed host.
	<i>service-name</i>	Name of an active SSG connection.
	<i>interface</i>	(Optional) The IP address through which the host is connected.

Defaults No default behavior or values

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
	12.2(2)B	The <i>interface</i> argument was added for the SSG Host Key feature.
	12.2(4)B	This command was modified to display information about SSG prepaid billing.

Examples

Prepaid Service Based on Volume Example

The following example displays the SSG connection for a prepaid service that uses a volume-based quota.

```
Router# show ssg connection 19.1.1.19 InstMsg
```

```
-----ConnectionObject Content -----
```

```
User Name:
Owner Host:19.1.1.19
Associated Service:InstMsg
Connection State:0 (UP)
Connection Started since:*00:25:58.000 UTC Tue Oct 23 2001
User last activity at:*00:25:59.000 UTC Tue Oct 23 2001
Connection Traffic Statistics:
    Input Bytes = 0, Input packets = 0
    Output Bytes = 0, Output packets = 0
    Quota Type = 'VOLUME', Quota Value = 100
Session policing disabled
```

Prepaid Service Based on Time Example

The following example displays the SSG connection for a prepaid service that uses a time-based quota.

```
Router# show ssg connection 19.1.1.22 Prepaid-internet
```

```
-----ConnectionObject Content -----
User Name:Host
Owner Host:19.1.1.22
Associated Service:Prepaid-internet
Connection State:0 (UP)
Connection Started since:*00:34:06.000 UTC Tue Oct 23 2001
User last activity at:*00:34:07.000 UTC Tue Oct 23 2001
Connection Traffic Statistics:
    Input Bytes = 0, Input packets = 0
    Output Bytes = 0, Output packets = 0
    Quota Type = 'TIME', Quota Value = 100
Session policing disabled
```

Autologin Service Example

The following example shows the service connection for the autologin service to host 10.3.6.1:

```
Router# show ssg connection 10.3.6.1 autologin
```

```
----- ConnectionObject Content -----
User Name:autologin
Owner Host:10.3.6.1
Associated Service:autologin
Connection State:0 (UP)
Connection Started since:
*20:41:26.000 UTC Fri Jul 27 2001
User last activity at:*20:41:26.000 UTC Fri Jul 27 2001
Connection Traffic Statistics:
    Input Bytes = 0 (HI = 0), Input packets = 0
    Output Bytes = 0 (HI = 0), Output packets = 0
```

Table 6 describes the significant fields shown in the display.

Table 6 *show ssg connection Field Descriptions*

Field	Description
User Name	Subscriber name supplied at authentication.
Owner Host	IP address of the subscribed host.
Associated Service	Service name of the connected service.
Connection State	State of activation (active or inactive).
Connection Started since	Time of host connection to the associated service.
User last activity at	Time of last data packet sent over this connection.
Input Bytes	Number of bytes received on this connection.
Input packets	Number of packets received on this connection.
Output Bytes	Number of bytes sent on this connection.
Output packets	Number of packets sent on this connection.
Quota Type	Form in which the quota value is expressed (time or volume).
Quota Value	Value of the quota (in bytes for volume or seconds for time).

Related Commands

Command	Description
clear ssg connection	Removes the connections of a given host and a service name.

Glossary

Access-Accept—Response packet from the RADIUS server notifying the access server that the user is authenticated. This packet contains the user profile, which defines the specific AAA functions assigned to the user.

Access-Request—Request packet sent to the RADIUS server by the access server requesting authentication of the user.

DHCP—Dynamic Host Configuration Protocol. Protocol that provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.

DNS—Domain Name Server. The part of the distributed database system used for resolving a fully qualified domain name into the four-part IP number used to route communications across the Internet.

SESM—Subscriber Edge Services Manager. Successor product to the Cisco SSD. The SESM is part of a Cisco solution that allows subscribers of digital subscriber line (DSL), cable, wireless, and dial-up to simultaneously access multiple services provided by different Internet service providers, application service providers, and Corporate Access Servers.

SNMP—Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SSD—The Service Selection Dashboard (SSD) server is a customizable Web-based application that works with the Cisco SSG to allow end customers to log on to and disconnect from proxy and pass-through services through a standard Web browser.

SSG—Service Selection Gateway.

VPDN—virtual private dial-up network. A VPDN is a network that extends remote access to a private network using a shared infrastructure. VPDNs use Layer 2 tunnel technologies (L2F, L2TP, and PPTP) to extend the Layer 2 and higher parts of the network connection from a remote user across an ISP network to a private network.