Cisco SSG-to-ISG DSL Broadband Migration Guide

First Published: April 27, 2005
Last Updated: January 21, 2009

Intelligent Service Gateway (ISG) is a Cisco IOS software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This document provides information and procedures to migrate broadband components from the Cisco Service Selection Gateway (SSG)—a Cisco IOS software feature set that works with the Cisco Subscriber Edge Services Manager (SESM) and other components to provide a subscriber edge services solution—to the Cisco Intelligent Service Selection Gateway (ISG) and updated SESM feature software.

This document is intended for network engineers migrating an SSG-based deployment to an ISG-based one. It is expected that the user of this document is knowledgeable about Cisco IOS and SSG software.

For this phase of SSG-to-ISG migration, only digital subscriber line (DSL) network migration has been tested and is supported. Migrating deployments such as wireless LAN (WLAN) and general packet radio service (GPRS) will be described at a later time in separate documents.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites

Cisco IOS ISG Feature Set

Cisco IOS software is packaged in feature sets that are supported on specific platforms. The Cisco ISG software is supported on Cisco 7200, 7300, and 10000 series routers. To get updated information regarding platform support and ISG feature sets, access Cisco Feature Navigator at http://www.cisco.com/go/fn.

To access Cisco Feature Navigator, you must have an account on Cisco.com. Qualified users can establish an account on Cisco.com by following the directions at http://www.cisco.com/register. If you have an account but have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you.

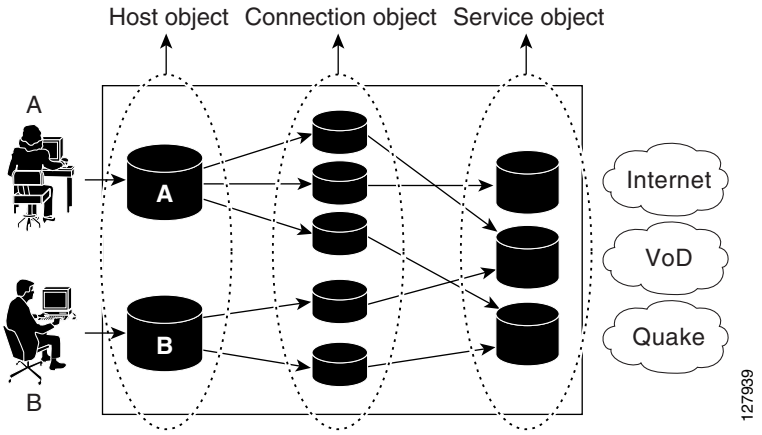
Backup Cisco IOS SSG Image

To be able to revert to your current SSG image, you must store your latest SSG configuration on a server. Once you load the ISG software and save a configuration, you will lose all SSG commands and all SSG references in the startup configuration file. To go back to an SSG image, reboot the router with the saved SSG image and load the stored SSG configuration from the server into the router again.

ISG Overview

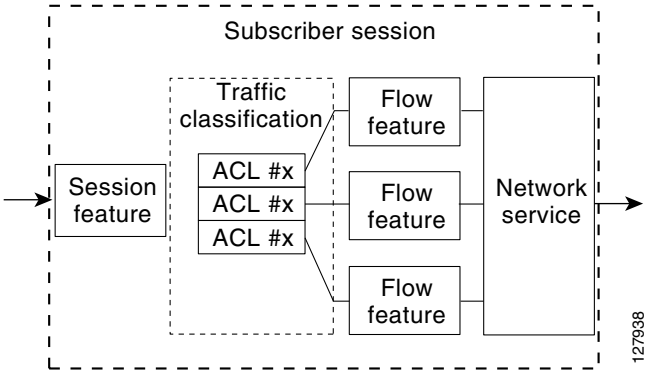
Figure 1 shows the SSG software architecture, where services are essentially a dynamic route that is installed for a subscriber when a given service is activated by combining a list of IP subnets with an uplink interface binding. Connections are destination-based only and do not take full advantage of routing capability available from the Cisco IOS software. Packets destined to and from the destination zone, as defined by a particular SSG service, are considered to flow through a service connection, and features associated with a particular service, that is, specified in the service profile, are applied only to those packets.

Figure 1 Cisco SSG Architecture



The ISG software provides a structured framework in which access edge devices can deliver flexible and scalable services to subscribers. Figure 2 shows the architecture that represents the new model for offering subscriber services from access edge devices. For the ISG, a service is a collection of features that are applicable to a subscriber session. The service is not necessarily associated with a destination zone or a particular uplink interface.

Figure 2 Cisco ISG Architecture



The traffic classification component of the ISG model is a set of criteria by which a traffic stream can be refined. A traffic class is specified by means of an access control list (ACL), and would be defined for, as an example, all User Datagram Protocol (UDP) packets or all packets destined to a particular subnetwork.

The network service is a forwarding mechanism that defines how packets are forwarded or received for a given session. Flow in the ISG software refers to a session's data stream as it has been identified by a classifier. The classifier categorizes data packets based on attributes of that packet, and classifiers are evaluated in a deterministic manner that ensures that a packet is assigned to exactly one category.

The result of configuring an ISG is a collection of powerful and dynamic policies that can be applied to the subscriber session. The new policies are a superset of the SSG concept of a service. With the ISG software, new subscriber rules allow you to build policies based on conditional events and by triggering service actions. Services can be implemented within virtual routing contexts.

The dynamic policy enforcement inherent in the ISG software allows consistent, tailored, and secure user services to be deployed in the network, triggered by a service or by a user—concepts referred to in the ISG as *push* and *pull*.

The ISG has the ability to initiate and manage sessions consistently, regardless of the access protocol type, network service, or session traffic policies configured. The ISG software provides seamless integration with existing Cisco IOS IP services such as Domain Name System (DNS), quality of service (QoS), ACLs, Dynamic Host Configuration Protocol (DHCP), VPN routing and forwarding (VRF) instances , and Multiprotocol Label Switching (MPLS).

The ISG software also provides better accounting of services for both use and application, and for advanced accounting for services such as prepaid. You will also find enhanced distributed conditional debugging that provides the ability to monitor and debug sessions and services based on identity.

ISG-SESM Broadband Migration Concepts

When migrating a network from SSG to ISG, the process is not a one-to-one mapping of commands but, rather, involves implementing the right policies to emulate the behavior on the Cisco SSG.

The following sections are provided to compare SSG-to-ISG functionality, identify similarities and differences, and introduce new concepts and commands that will help you move to the ISG architecture.

ISG Features

An ISG feature is a functional component that performs a specific operation on a session's data stream. A feature may or may not be associated with a classifier. However, once associated with a classifier, a feature can be applied only to the packets that match that classifier. Otherwise, the feature is applied to all packets for that session. Features are divided into data-path and nondatapath-related functionality. Datapath-related features include Port-Bundle Host Key (PBHK), Layer 4 (L4) Redirect, Subscriber ACLs, Idle Timer, Session Timer, QoS, Session and Service Accounting, and Prepaid. Nondatapath-related features include IP configurations (address pool, VRF, IP address), and network service types or groups.

Dynamic Feature Updates

The ISG software supports dynamic updating of features for an existing ISG session. This update can be triggered by the actions of either a subscriber or an administrator. Once a session has been updated in this way, any existing configuration for the given feature is overridden, and the updated configuration can be altered only by another dynamic feature update.

SSG and ISG Services

A service on the SSG is a dynamic destination route that is installed for a subscriber when a given service is activated. Uplink commands are required to bind a service to an interface, and to indicate to the SSG where to find the destination route.

A service on the ISG is a collection of features that are applied to a subscriber session, with a session defined as a set of states associated with traffic for a single subject such as a user, client, subscriber, router, or interface. Unlike the SSG, there is no concept of binding a service to an interface on the ISG. An ISG service is not necessarily associated with a destination zone or a particular uplink interface and, therefore, makes no attempt to override the routing functionality provided by the Cisco IOS software. Because ISG services use Cisco IOS routing software, the services inherit routing capability like uplink redundancy, load-balancing across uplink interfaces, and MPLS integration. In this way, ISG services become value-added bundles that are more intuitive than SSG services.

The ISG software introduces the concept of network services, of which there are two types: packet forwarding and packet routing. A network service can be specified in a user profile and on an interface. For each subscriber session, only one instance of a network service can be specified at any point in time. The type of network service that is selected depends upon the presence of either a VRF-related or virtual private dialup network (VPDN) attribute in what is called a *primary service*.

When a network policy is included in a service profile or service policy map, the service is known as a primary service. Primary services are mutually exclusive, that is, only one instance of a network policy containing a primary service can be active per subscriber. The ISG software also offers nonprimary services, which can have dependencies on primary services. Both primary and nonprimary services can be configured remotely in a profile, or locally on the router.

ISG Policies

A service profile on the ISG software includes event policy control using control policy maps. The policy maps control what actions are triggered for the subscriber using an event and class combination. The ISG software can also control traffic inside the flow and take specific measures on the traffic using service policy maps. The service policy maps make decisions about what actions to take on the traffic and are triggered by a control policy map. For example, it is a policy that associates a feature with a classifier. A service policy map combines an action and a feature. Service policies can be configured both remotely (in most cases), and locally.

A control policy map is a collection of rules that describe what action to take under what circumstances. It is declared from a set of predefined events, operands, match operators, and actions that provide precise rules of behavior. These declarations can be defined in many ways to provide powerful solutions to the needs of the service provider. A control class builds the conditions that identify particular characteristics of the subscriber session, and has an extensive list of classifications that can be used to identify session characteristics such as authentication, domain name, media, port, protocol, address, and username. A control policy map combines an event and an action. Control policies are configured locally using ISG commands.

ISG Traffic Classes

The ISG traffic class allows classification of session traffic into individual flows, and the application of other features on these flows. The traffic class creates instances for each of the traffic flows belonging to a subscriber, which allows the session-related capabilities of the ISG software to be applied on these flows.

All features configured in a traffic class service profile are applied to the flow defined by ACLs. Multiple traffic class service profiles with various features can be applied to a session. The service profile includes the direction, either inbound or outbound, to which the ACL is applied, and the priority of the traffic class. The priority is used to determine which ACL is first used for the match. Once a match is made, features defined in the traffic class service profile will be executed for that traffic class. Packets that do not match any of the ACLs are considered to be part of default traffic and are processed as if a traffic policy was not applied to the session. When a packet matches more than one traffic class, it is classified in the class with the highest priority. Features in the latest applied service profile with overlapping classification information, as in an earlier service profile, are given priority. Additionally, any traffic class you define receives the highest priority when no priority is given and, if you have overlapping destinations in several traffic classes applied to a subscriber's session, the traffic will always match the traffic class that has been applied the longest to the session.

The default behavior of traffic class services can be changed such that all default traffic is dropped. One of the first migration tasks described later in this document is to make sure that, for all PPP over Ethernet (PPPoE) sessions, you restore the default SSG behavior of dropping an unauthenticated packet by inserting a traffic drop action in a traffic class. A service policy map or service profile that contains a traffic class is called a traffic policy. Although you can specify the events that trigger an ISG control policy, the trigger for a traffic policy is the arrival of a data packet.

Besides local traffic class policies, traffic classification can be configured remotely in a RADIUS profile using Cisco attribute-value (AV) pairs and in ACLs that have been configured on the ISG.

SSG-to-ISG Feature Map

Once you load the ISG software, you will remove all SSG commands and configurations. No automatic conversion is done to restore SSG functionality with ISG commands. Use Table 1 to help you map SSG-to-ISG features. Find the Cisco IOS documentation section listed in Table 1 in either the *ISG Configuration Guide* or in this document. If you are viewing an electronic version of this document, click the highlighted titles to display information about a feature.

Table 1 SSG-to-ISG Feature Map

ISG Feature	Cisco IOS Documentation Section	Related SSG Feature
Accounting		
• Per Session, Service, and Flow • Postpaid	• *Configuring ISG Accounting* chapter • "ISG Tariff Switching: Postpaid Services" section on page 79 in this document	• SSG Accounting • RADIUS Accounting Records Used by SSG • Postpaid Tariff Switching
• Prepaid • Tariff Switching	• *Configuring ISG Support for Prepaid Billing* chapter • "Configuring Prepaid Service" section on page 33 in this document • "SSG-to-ISG Migration of Prepaid and Postpaid Services Examples" section on page 50 in this document	• SSG Prepaid • Prepaid Tariff Switching

Table 1 SSG-to-ISG Feature Map (continued)

ISG Feature	Cisco IOS Documentation Section	Related SSG Feature
Flow Control		
• Flow Redirect	• *Redirecting Subscriber Traffic Using ISG Layer 4 Redirect* chapter • "Configuring Layer 4 Redirect" section on page 26 in this document • "Configuring Advertisement and Initial Redirection" section on page 39 in this document	• Redirection for Unauthenticated Users • Redirection for Unauthorized Services • Initial Captivation • TCP Redirect Access Control Lists • Permanent TCP Redirection • DNS Redirection
• Dynamic Rate Limiting	• *Configuring ISG Policies for Regulating Network Access* chapter	• Hierarchical Policing
Policy Control		
• Service Profiles	• *Configuring ISG Subscriber Services* chapter	• Services and Service Profiles
• DHCP Proxy	• *Configuring ISG Access for IP Subscriber Sessions* chapter	• —
• Cisco Policy Language • Multidimensional Identity per Session • Domain Based (Auto-domain, Proxy) • Triggers (Time, Volume, Duration)	• *Configuring ISG Control Policies* chapter • "Configuring Pass-Through and Proxy Services in a RADIUS Profile" section on page 28 in this document	• —
• CoA	• *Enabling ISG to Interact with External Policy Servers* chapter	• —
Sessions		
• Port-Bundle Host Key	• *Configuring ISG Port-Bundle Host Key* chapter • "Configuring ISG and SESM Interoperability" section in this document	• SSG Port-Bundle Host Key • SSG Port-Bundle Host Key Functionality and Local Forwarding
• Transparent Autologon	• "Uses of Control Policies" section of the *Configuring ISG Control Policies* chapter	• SSG Transparent Autologon
• Per-Service Idle Timeout	• *Configuring ISG Policies for Session Maintenance* chapter	• SSG Session Timeout and Idle Timeout

Table 1 SSG-to-ISG Feature Map (continued)

ISG Feature	Cisco IOS Documentation Section	Related SSG Feature
• L2/L3 Interface IP Session • Protocol Event (DHCP)	• *Configuring ISG Layer 3 Access* chapter	• Configuring SSG Interface Direction
• VRF Transfer	• *Configuring ISG VRF Transfer* chapter	• —
• Single Sign-On	• *Overview of ISG* chapter • "Single Sign-On in the ISG" section on page 16 in this document	• Configuring SSG to Authenticate PPP Subscribers
Network Interface		
• IP Routed • VRF-Aware MPLS • L2TP	• *Configuring ISG Network Forwarding Policies* chapter	• —
Monitoring and Debugging		
• Advanced Conditional Debugging • Session and Flow Monitoring	• *Troubleshooting ISG with Session Monitoring and Distributed Conditional Debugging* chapter	• —

RADIUS Profile Migration

One change for RADIUS profiles used by the ISG is that a more verbose style for defining attributes than was accepted in the SSG has been developed. The verbose style was adapted because it is self-documenting and more easily extended than the one- or two-letter cryptic formats used for RADIUS profiles on the SSG. Remember, however, that this change pertains only to those attributes used to define ISG-specific profiles. The ISG will continue to interpret SSG-equivalent user profile-related attributes, attributes that are interpreted by the SESM service selection web page, and vendor-specific attributes (VSAs) in accounting messages and prepaid authorization requests.

The following sections provide more specific details about the RADIUS profiles used by the SSG and the ISG:

Service Profiles

Service profiles continue to be used by the ISG to define the services that subscribers can select from SESM service selection web page, as is the case for the SSG. Existing SSG service profiles can be reused on the ISG, although it may be necessary to add ISG attributes to the existing set of SSG service profiles. The SESM service selection web page and the SSG will read the legacy attributes and ignore the new attributes and, conversely, the ISG will read only the new attributes and ignore the legacy attributes.

There are a couple of exceptions to this; see the notes about attributes that must remain in service profiles for ISG-SESM interoperability in the "SESM Requirements for RADIUS Service Profile Attributes" section on page 16. Also, on the SSG the number of services a subscriber can have is limited with the **ssg maxservice** command, and this command is not available on the ISG.

Service Group Profiles

Service group profiles are used only by the SESM service selection web page to identify a list of services belonging to a specific service group. That service group is, therefore, used only by the SESM service selection web page; the attributes to define the service group do not need to be converted in any way to allow the attributes to be interpreted by the ISG. No migration effort is required to adapt these specific profiles in a network topology with ISGs.

Subscriber and User Profiles

Subscriber and user profiles defined for the SSG remain the same for the ISG, and continue to define logon names and passwords, ACLs associated with each logon, and subscribed services for each logon.

Next Hop Gateway and Tunnel Service Profiles

Next hop gateway profiles are not used on the ISG. These profiles associate next hop gateway keys with IP addresses, and this service binding concept is not used on the ISG.

It is not possible for the ISG to convert tunnel service profiles used under SSG.

RADIUS Service and User Profile Attributes

Table 2, Table 3, and Table 4 list the SSG RADIUS and VSA attributes that are interpreted by the ISG and that are new for the ISG. If the attribute is still interpreted by the ISG, it is used in the same manner as on the SSG, as indicated in the "SSG Uses?" and "SSG Sends?" columns of Table 2. See configuration examples in this document and the *ISG Configuration Guide*, to learn more about the new attributes used to define ISG-specific profiles.

Table 2 RADIUS Service and User Profile Attributes

Attribute Type	Attribute Code	Function, or ISG Equivalent if Not Interpreted	Interpreted by ISG?	In User Profiles?	In Service Profiles?	In Service Group Profiles?	Accounting Required?	Prepaid Service Authorization and Reauthorization	SESM Uses?	SESM Sends?	SSG Uses?	SSG Sends?
Account-Info	A*activate-service-name*	Automatically activates the named service.	Yes	Yes	No	No	No	No	No	No	Yes	No
Account-Info	N*service-name*	Makes service name available to subscriber.	Yes	Yes	No	Yes	No	No	Yes	No	No	No
Account-Info	Q[U|D]	QoS parameters for the session in both the Upstream and Downstream direction (feature push capabilities).	Yes	Yes	No	No	No	No	No	No	Yes	No
Account-Info	V*cookie*	Specifies a cookie string for a service.	Yes	Yes	No	No	Yes	No	No	No	No	No
Account-Info	H*url*	Used only by SESM. Subscriber home page URL requested when the service is activated using the service selection web page.	No	Yes	No	No	No	No	Yes	No	No	No
Account-Info	$AA	Used only by SESM.	No	Yes	No	No	No	No	Yes	No	No	No
Account-Info	$FA	Used only by SESM.	No	Yes	No	No	No	No	Yes	No	No	No
Account-Info	$GA	Used only by SESM.	No	Yes	No	No	No	No	Yes	No	No	No
Account-Info	$GA	Used only by SESM.	No	Yes	No	No	No	No	Yes	No	No	No
Account-Info	$GB	Used only by SESM.	No	Yes	No	No	No	No	Yes	No	No	No
Account-Info	$PE	Used only by SESM.	No	Yes	No	No	No	No	Yes	No	No	No
Account-Info	$SA	Used only by SESM.	No	Yes	No	No	No	No	Yes	No	No	No
Account-Info	$SB	Used only by SESM.	No	Yes	No	No	No	No	Yes	No	No	No
Account-Info	$SL	Used only by SESM.	No	Yes	No	No	No	No	Yes	No	No	No
Account-Info	$UG	Used only by SESM.	No	Yes	No	No	No	No	Yes	No	No	No
Account-Info	G*group-name*	Used only by SESM. Specifies that subscriber can make use of this service group.	No	Yes	No	No	No	No	Yes	No	No	No
Account-Info	I*group-name*	Used only by SESM. Specifies name of service group to SESM.	No	No	No	Yes	No	No	Yes	No	No	No

Table 2 RADIUS Service and User Profile Attributes (continued)

Attribute Type	Attribute Code	Function, or ISG Equivalent if Not Interpreted	Interpreted by ISG?	In User Profiles?	In Service Profiles?	In Service Group Profiles?	Accounting Required?	Prepaid Service Authorization and Reauthorization	SESM Uses?	SESM Sends?	SSG Uses?	SSG Sends?
Account-Info	TE	Used only by SESM. Specifies whether services in a service group are mutually exclusive.	No	No	No	Yes	No	No	Yes	No	No	No
Account-Info	R[I|S|A]	In SSG, specifies TCP redirection for SMTP, initial captivation, or advertisement. See the "Configuring Advertisement and Initial Redirection" section on page 39 for more information.	No	Yes	Yes	No	No	No	No	No	Yes	No
Account-Info	S[*IP-address* | *PBHK*]	Subscriber identifier attribute.	Yes	Yes	No	No	No	No	Yes	Yes	Yes	Yes
Service-Info	Q[U|D]	Uplink and downlink subscriber policing (feature push capabilities).	Yes	No	Yes	No	No	No	No	No	Yes	No
Service-Info	B	MTU for SSG L2TP service.	No	No	Yes	No	No	No	No	No	Yes	No
Service-Info	E	Maximum service connections.	No	No	Yes	No	No	No	No	No	Yes	No
Service-Info	H	Used only by SESM.	No	No	Yes	No	No	No	Yes	No	No	No
Service-Info	N	Used only by SESM.	No	No	Yes	No	Yes	Yes	Yes	No	No	No
Service-Info	D	DNS server name.	No	No	Yes	No	No	No	No	No	Yes	No
Service-Info	G	Next hop gateway (service route); this SSG service concept is obsolete on ISG.	No	No	Yes	No	No	No	No	No	Yes	No
Service-Info	I	Used only by SESM. Service name to be displayed on SESM.	No	No	Yes	No	No	No	Yes	No	No	No
Service-Info	M[C|S]	Sequential service can be done using class control in a policy map where one service-start function causes another to stop.	No	No	Yes	No	No	No	Yes	No	Yes	No
Service-Info	O	Service domain.	No	No	Yes	No	No	No	No	No	Yes	No
Service-Info	PPW:*tariff time*:*days*	Postpaid tariff switch parameters.	Yes	No	Yes	No	No	No	No	No	Yes	No

Table 2 RADIUS Service and User Profile Attributes (continued)

Attribute Type	Attribute Code	Function, or ISG Equivalent if Not Interpreted	Interpreted by ISG?	In User Profiles?	In Service Profiles?	In Service Group Profiles?	Accounting Required?	Prepaid Service Authorization and Reauthorization	SESM Uses?	SESM Sends?	SSG Uses?	SSG Sends?
Service-Info	PZS*prepaid-server-definition* PZI*value*	SSG prepaid subattributes. PZS defines prepaid server details to use for authorization. PZI is used for interim accounting. On the ISG, replace PZS with VSA 'prepaid-config= *prepaid-config- nam*e'. PZI is not supported on ISG.	No	No	Yes	No	No	No	No	No	Yes	No
Service-Info	R	Use traffic class. ACLs for traffic class must be defined on ISG and match the R value.	No	No	Yes	No	No	No	Yes	No	Yes	No
Service-Info	S	Service-info code for RADIUS server used for remote authentication. Replace with Cisco AV pair "subscriber:policy-directive"	No	No	Yes	No	No	No	No	No	Yes	No
Service-Info	T[X|T|P]	Type of service: proxy (X), tunnel (T), or pass-through (P). The SSG service concept is obsolete on the ISG.	No	No	Yes	No	Yes	No	Yes	No	Yes	No
Service-Info	Z	Prepaid service on SSG. On ISG, this attribute is replaced with the Cisco AV pair "prepaid-config= *name*" where *name* is the prepaid configuration named on the ISG. By default, there is always a default configuration name present on the ISG named default.	No	No	Yes	No	No	No	No	No	Yes	No
Service-Info	V*cookie*	Service cookie.	Yes	No	Yes	No	No	No	No	No	Yes	No

Table 2 RADIUS Service and User Profile Attributes (continued)

Attribute Type	Attribute Code	Function, or ISG Equivalent if Not Interpreted	Interpreted by ISG?	In User Profiles?	In Service Profiles?	In Service Group Profiles?	Accounting Required?	Prepaid Service Authorization and Reauthorization	SESM Uses?	SESM Sends?	SSG Uses?	SSG Sends?
Service-Info	L*interval*	Accounting update interval. See the "SSG and ISG Accounting and RADIUS Update Examples" section on page 42 for more information.	No	No	Yes	No	No	No	No	No	Yes	No
Service-Info	U*name*	Service user name included in accounting requests.	Yes	No	Yes	No	Yes	No	No	No	Yes	No
Service-Info	X	Appends the service name to the username during authentication as *username*@*servicename*.	No	No	Yes	No	No	No	No	No	Yes	No
Control-Info	QT*value* QV*value* QR*number* QB*bytes-used since-switch* QX*seconds*; *bytes*;*bytes*	QT defines TimeQuota. QV defines Volume-based Quota. QR defines Prepaid ReauthReason. QB defines VolumeQuota (new allocation). QX defines QuotaPostSwitch. Function and use of these attributes remain the same for ISG as on SSG.	Yes	No	Yes	No	Yes	Yes	No	No	Yes	Yes
Control-Info	I*value-overflow*; *value*	Indicates the overflow value and value of I (input) bytes in accounting packets. The formula to calculate the exact byte count is *value-overflow**4294967296 + *value*.	Yes	No	No	No	Yes	No	No	No	No	Yes

Table 2 RADIUS Service and User Profile Attributes (continued)

Attribute Type	Attribute Code	Function, or ISG Equivalent if Not Interpreted	Interpreted by ISG?	In User Profiles?	In Service Profiles?	In Service Group Profiles?	Accounting Required?	Prepaid Service Authorization and Reauthorization	SESM Uses?	SESM Sends?	SSG Uses?	SSG Sends?
Control-Info	O*value-overflow*; *value*	Indicates the overflow value and value of O (output) bytes in accounting packets. The formula to calculate the exact byte count is *value-overflow**4294967296 + *value.*	Yes	No	No	No	Yes	No	No	No	No	Yes
Control-Info	XP*domain*	Only present in Access-Accept when SSG queries the RADIUS server for the list of domains to exclude with the PTA-MD exclusion feature.	No	No	No	No	No	No	No	No	Yes	No
Control-Info	G*name; IP-address*	Defines a table of keys and IP addresses that will be used as next hop gateway routers.	No	No	Yes	No	No	No	No	No	Yes	No

Table 3 Supported RADIUS IETF Attributes

Attribute	Description
Filter-Id= *value*	For feature push. A message can contain a reference to an existing ACL definition using Filter-Id as a key and the value as the reference name to the ACL definition.
Session-Timeout=*seconds*	Standard RADIUS attribute number 27. When inserted in a subscriber profile, this attribute specifies the maximum length of time, in seconds, that the subscriber session can remain active at any one time on the ISG. When inserted in a service profile, this attribute specifies the maximum length of time, in seconds, that the service the subscriber has subscribed to can remain active before being disconnected from the service.
Idle-Timeout=*seconds*	Standard RADIUS attribute number 28. When inserted in a subscriber profile, this attribute specifies the maximum length of time, in seconds, that a subscriber session can remain idle before it is disconnected. When inserted in a service profile, this attribute specifies the maximum length of time, in seconds, that the service the subscriber has subscribed to can remain idle before being disconnected from the service.

Table 4 New and Existing VSA Attributes Supported on the ISG

Cisco Attribute Type	Cisco Attribute Code	Description
Existing SSG Attributes Supported on the ISG		
Cisco-AVpair	ip:inacl[#*number*]={*standard-access-control-list* | *extended-access-control-list*}	Incoming ACL definition, for feature push.
Cisco-AVpair	ip:outacl[#*number*]={*standard-access-control-list* | *extended-access-control-list*}	Outgoing ACL definition, for feature push.
Cisco-AVpair	ip:pool-def#	IP pool definition.
Cisco-AVpair	ip-addr pool	IP address pool name.
New ISG Attributes		
Cisco-AVpair	subscriber:accounting-list=*accounting-method-list-name*	The service requires accounting.
Cisco-AVpair	subscriber:policy-directive=authenticate on aaa list	The service requires authentication.
Cisco-AVpair	subscriber:*vrf-id*	Identifier for the virtual routing table.
Cisco-AVpair	subscriber:*subscriber-service*	Type of service—**vpdn**, **local**, **deny**, or **relay-pppoe**.
Cisco-AVpair	subscriber:service-type=*primary*	Indicates whether service is primary.
Cisco-AVpair	subscriber:service-group=*group-name*	Defines a group name to outline what nonprimary services are dependent on a primary service.
Cisco-AVpair	ip:traffic-class= [in | out] *access-group* [*acl-number* | *acl-name*]	Classification for defining a flow for a traffic class. **Note** ACL cannot be dynamically downloaded via the ip:inacl or other VSA pairs. The ACLs in this command must be predefined on the ISG.
Cisco-AVpair	ip:l4redirect	Enables L4 redirection.
Cisco-AVpair	ip:portbundle=enable	Enable PBHK as the session identifier.

ISG-SESM Interoperability

The client-server relationship between the SESM service selection web page as RADIUS client and the Cisco gateway (both the SSG and ISG) as RADIUS server remains the same. Additionally, changes to SESM configuration are not required when migrating to ISG. Read through the following sections, however, to understand other changes that you may need to make to establish ISG-SESM interoperability.

Restoring ISG-SESM interoperability is described in the "Configuring ISG and SESM Interoperability" section on page 23.

Supported SESM Version

Version 3.2(2) of SESM software has been verified to work in the ISG.

SESM Requirements for RADIUS Service Profile Attributes

SESM activates only those subscriber services that include the R attribute in the authentication, authorization, and accounting (AAA) RADIUS profiles. The R attribute is required in service profiles on both the SSG and ISG that define subscriber services that will be exposed in the SESM service selection web page However, nonsubscriber services that are defined only on the ISG itself and will not be exposed in the SESM service selection web page, such as PBHK and L4 redirection, are defined in a service profile without the R attribute.

The TX attribute is also required in proxy service profile definitions on the ISG; otherwise SESM will not manipulate the proxy service definitions correctly and the service login page will not be presented.

No Default Network

The concept of a default network does not exist in the ISG, and SESM is not installed in a default network on the ISG.

RPC Messaging Principles

There are no changes to the remote procedure call (RPC) messaging principles between the ISG and SESM; that is, service logon, logoff, user logon, user logoff, and account-query all remain RADIUS-based.

Although a new Change of Authorization (CoA) RFC3576-based policy and portal server communication model is introduced in the ISG software, for backward compatibility, the ISG can also operate in traditional SSG-SESM RPC mode. Describing the new CoA model is beyond of the scope of this document. See the "Overview of ISG" chapter in the *Cisco IOS Intelligent Service Gateway Configuration Guide* for more information.

Single Sign-On in the ISG

Single Sign-On (SSO) functionality also remains the same for the ISG. As with the SSG, the SSO feature in the ISG eliminates the need to authenticate a session more than once, and allows subscribers to close the SESM service selection web page or navigate away from selection web pages and return later without the need to reauthenticate.

The ISG SSO feature can be configured on ATM ports implementing RFC1483 bridging. When ports are configured for RFC1483 bridging, the initial state is set to unauthenticated and no subscriber data except authentication traffic is allowed through the port. The router authenticates the end user using RADIUS

by taking the username and password from the Account Logon request. Once the end user is authenticated, the port state transitions into the authenticated state and no further authentication is required for subsequent connections.

One of the key elements of SSO using RFC1483 bridging is the query sent by SESM to obtain the authenticated state of the session from the ISG device. This query is done using a RADIUS request with the appropriate attributes added to the Access-Request. The ISG software contains a limited-feature RADIUS server to answer this query by sending an appropriate Access-Response containing attributes indicating the state of the session. The "Configuring ISG and SESM Interoperability" section on page 23 shows how to enable a limited-feature RADIUS server to allow the ISG to answer the Account Logon request from SESM.

ISG Session Disconnect

The initial steps in the "Configuring ISG and SESM Interoperability" section on page 23 describe the configuration that allows the exchange of RADIUS protocol messages between the SESM and the ISG, and restores the RPC channel and SSO functionality between the ISG and SESM.

The exchange of RADIUS protocol messages between SESM and the SSG and ISG remains unchanged. But there are differences in how SESM handles session disconnects: In the SSG environment, when the log out button is pressed on the SESM web page, the SSG host object is terminated but the PPPoE session remains connected. In the ISG-SESM environment, pushing the log out button on the SESM web page disconnects the user's PPPoE session, and the session will need to be brought up again when the user next wants to log in.

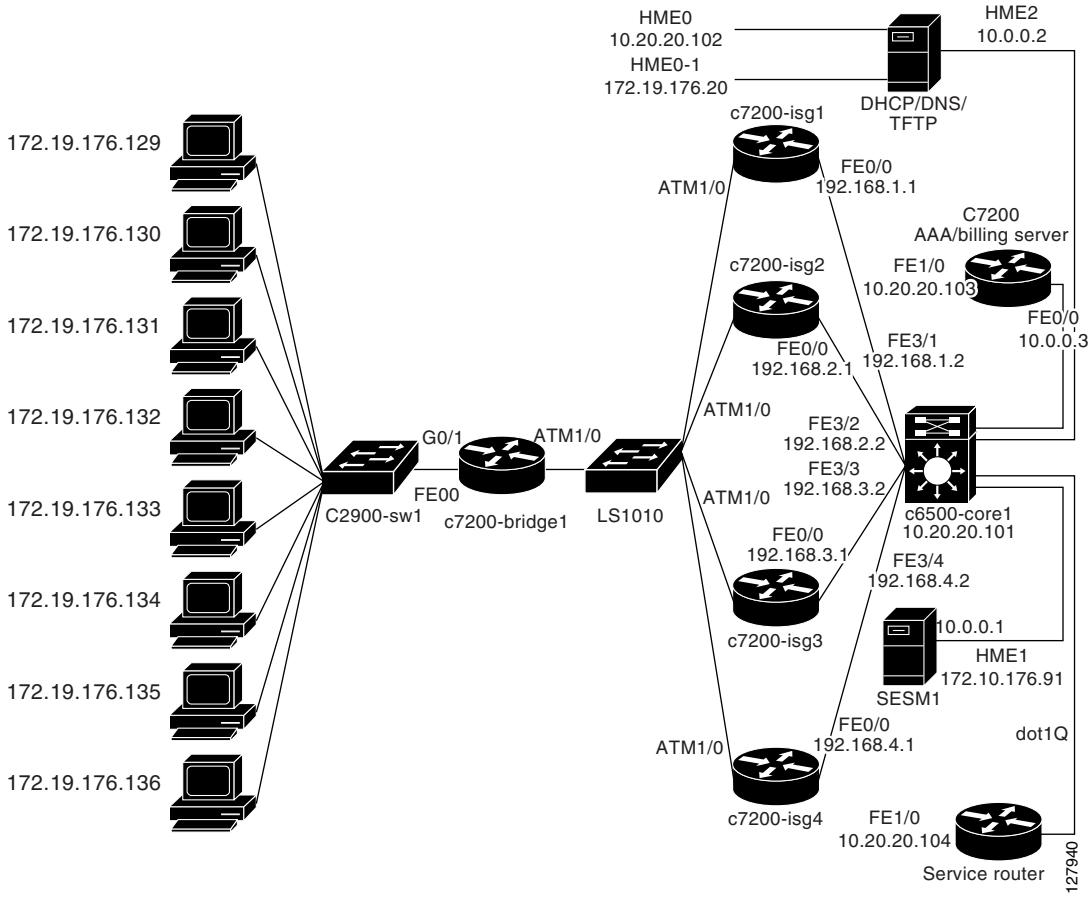
Basic ISG-SESM DSL Broadband and SSG-to-ISG Conversion Tasks

This section provides the following configuration tasks that establish basic ISG functionality and, in some cases, restore SSG functionality:

Cisco ISG Sample Topology

The conversion tasks in this section were defined for the network depicted in Figure 3. See the "ISG Network Configuration Example" section on page 91 for the running configuration of this network.

Figure 3 ISG Sample Topology



Configuring a Traffic Drop Policy

For this task, it is assumed that the SSG has an implicit drop policy for all traffic that does not match the IP address configured by either an R attribute statement in a service profile or in the **ssg default-network** command. Perform the steps in this section to make certain that for all PPPoE sessions the default traffic behavior of the SSG is restored.

Step 1 Use the **policy-map type control** command to associate the PPPoE session with a policy control map (named example-map1 in the sample running configuration):

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# policy-map type control example-map1
Router(config-control-policymap)# exit

Router(config)# interface Virtual-Template1
Router(config-if)# service-policy type control example-map1
```

Step 2 Define specific actions that need to be triggered when the session starts on the policy control map configured in Step 1. One of these actions must be to configure the traffic class that will allow traffic sent from the customer premises equipment (CPE) side of the network to pass when the IP destination of the traffic is targeted for the default network. Start by adding an action on the policy control map, under the session-start event in class control configuration mode. The action for the configuration executes a service named example_network_service.

```
Router(config)# policy-map type control example-map1
Router(config-control-policymap)# class type control always event session-start
Router(config-control-policymap-class-control)# 1 service-policy type service name
example_network_service
```

Step 3 Configure a service policy map to reconstruct the default network behavior found in the SSG so it will drop all traffic sourced from the CPE side with IP destinations something other than the default network. Use the **class-map type traffic** command to configure the traffic class map that will be used in the service policy:

```
Router(config)# class-map type traffic match-any traffic_class_example_network_service
Router(config-traffic-classmap)# match access-group in 110
Router(config-traffic-classmap)# match access-group out 111
Router(config-traffic-classmap)# exit
Router(config)# access-list 110 permit ip any 10.0.0.0 0.0.0.255
Router(config)# access-list 111 permit ip 10.0.0.0 0.0.0.255 any
Router(config)# policy-map type service example_network
Router(config-service-policymap)# class type traffic traffic_class_example_network_service
Router(config-service-policymap-class-traffic)#
```

Note The traffic class map must exist before being applied in a service policy map; otherwise, you will receive the message: %Warning: class-map "*name*" does not exist.

At this point, a traffic classification map has been configured on the service. The configuration prompt has changed to indicate that additional actions are possible on the traffic flow matching the traffic class map named traffic_class_example_network. You can use the **?** command to see additional actions that are possible.

```
Router(config-service-policymap-class-traffic)# ?
traffic-policy-map-classmap commands:
  accounting  Configure accounting parameters
  default     Set a command to its defaults
  exit        Exit from policymap-classmap service configuration mode
  no          Negate a command or set its defaults
  police      Police QoS Info
  redirect    Redirect rules
  timeout     Timeout parameters
```

Step 4 Enter the **exit** command to return to the config-service-policymap mode:

```
Router(config-service-policymap-class-traffic)# exit
```

Step 5 Define a policy that drops all other traffic not matching the traffic class named traffic_class_example_network. Each service policy map has a predefined default traffic class where the drop action is enabled. Use the **class type traffic default in-out** command to begin this definition, and set **drop** as a default action.

```
Router(config-service-policymap)# class type traffic default in-out
Router(config-service-policymap-class-traffic)# ?
traffic-policy-map-classmap default commands:
  default  Set a command to its defaults
  drop     action drop
```

```
  exit     Exit from policymap-classmap-def service configuration mode
  no       Negate a command or set its defaults

Router(config-service-policymap-class-traffic)# drop
Router(config-service-policymap-class-traffic)# exit
Router(config-service-policymap)# exit
```

Step 6 The service policy map defined in Step 3 can be configured either locally or on a RADIUS server. This step defines a new AAA method list on the ISG to indicate whether the service policy map resides locally or remotely. Use the **aaa new-model** and **aaa authorization** global configuration commands to make the definition. For this configuration, the AAA method list is found locally.

```
Router(config)# aaa new-model
Router(config)# aaa authorization subscriber-service default local
```

Verifying the Traffic Drop Policy

Perform the steps in this section to verify the traffic drop policy.

Step 1 With a PPPoE session up and running, use the **show subscriber session** command to verify the actions and events that were defined under the policy control map, as follows:

```
Router# show subscriber session username user-group3

Subscriber session handle: 9F00007C, state: connected, service: Local Term
Unique Session ID: 238
Identifier: user-group3
SIP subscriber access type(s): PPPoE/PPP
Root SIP Handle: FA00007B, PID: 187
Child SIP Handle: 6E000012, PID: 189
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:24:00, Last Changed: 00:24:00
AAA unique ID: 226
Switch handle: CA0ED
Interface: Virtual-Access4

Policy information:
  Authentication status: authen
  User profile, excluding services:
    service-type         2 [Framed]
  Active services associated with session:
    name "example_network_service"
  Prepaid context: not present

  Rules, actions and conditions executed:
    subscriber rule-map example-map1
      condition always event session-start
        action 1 apply service example_network_service
.
.
.
```

For every action that was triggered in the service policy map, there will be a similar report that describes the subscriber session output.

Tip Before this information can be displayed, the default recording function must be enabled. The recording function has a history limit of 64 rules, and can be disabled with the **no subscriber policy recording rule** global configuration command.

Step 2 To determine which policy control map is associated with a session when recording is disabled, enter the **show caller** command to determine the line number, and the **show interfaces virtual-access** command to display the configuration, as follows:

```
Router# show caller
                                                 Active    Idle
  Line           User               Service      Time      Time
  con 0          -                  TTY          00:00:10  00:00:00
  Vi2.1          user-group3        PPPoE        06:47:58  02:22:33


Router# show interfaces virtual-access 2.1 configuration

Virtual-Access2.1 is a PPP over Ethernet link (sub)interface

Derived configuration : 318 bytes
!
interface Virtual-Access2.1
 ip unnumbered Loopback0
 ip mtu 1492
 service-policy type control example-map1
 ppp authentication chap
end
```

Testing the Traffic Drop Policy

The steps in this section describe how you can test the traffic drop policy.

Step 1 If the policy control map was applied successfully, test it by repeating a ping test from the CPE client to the web server. Also use the **ping** command to test a connection to an IP address in the default network, either the SESM service selection web page or the RADIUS server.

Step 2 The **show subscriber session** command provides several options for displaying specific session details. Use of a traffic class on the ISG initiates the creation of a unique identifier (uid) that can be displayed by entering the **show subscriber session** command. Enter the **show subscriber session** command again with the uid to see session details.

To verify that the drop policy has been configured correctly and to see if packets have been dropped, enter the **show subscriber session** command with the username. The following examples show the type of information displayed by these commands:

```
Router# show subscriber session

Current Subscriber Information: Total sessions 1

Uniq ID Interface  State         Service      Identifier          Up-time
42      Vi2.1      authen        Local Term   user-group3         00:00:10
43      Traffic-Cl connected     Ltm Internal                     00:00:10
```

```
Router# show subscriber session uid 43

Subscriber session handle: 6B0000A0, state: connected, service: Ltm Internal
Unique Session ID: 43
Identifier:
SIP subscriber access type(s): Traffic-Class
Root SIP Handle: CF00001E, PID: 98
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:00:17, Last Changed: 00:00:17
AAA unique ID: 0
Switch handle: 402A

Configuration sources associated with this session:
Service: example_network_service, Active Time = 00:00:17
```

Because traffic class flows are no longer modeled as separate sessions, they do not show up that way in the output of this command. The traffic class flow features appear in the output of the parent session, rather than under a separate traffic class session. In the following example, key packet and drop policy information is indicated in bold text for purpose of example:

```
Router# show subscriber session username user-group3

Unique Session ID: 220
Identifier: user-group3
SIP subscriber access type(s): PPPoA/PPP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:59:59, Last Changed: 00:17:45
AAA unique ID: 211
Interface: Virtual-Access4

Policy information:
  Context 2078F3B0: Handle 6C000041
  Authentication status: authen
  Active services associated with session:
    name "DEFAULT"
    name "PBHK"
  Rules, actions and conditions executed:
    subscriber rule-map DEFAULT_RULE_MAP
      condition always event session-start
        1 authenticate aaa list CAR
        2 service-policy type service name PBHK
        3 service-policy type service name DEFAULT

Session inbound features:
Traffic classes:
  Traffic class session ID: 221
   ACL Name: DEFAULT_IACL, Packets = 126, Bytes = 12392
 Default traffic is dropped
 Unmatched Packets (dropped) = 0, Re-classified packets (redirected) = 0

 Feature: Portbundle Hostkey
 Portbundle IP = 10.10.100.7     Bundle Number = 70

Session outbound features:
Traffic classes:
  Traffic class session ID: 221
   ACL Name: DEFAULT_OACL, Packets = 206, Bytes = 184863
 Default traffic is dropped
 Unmatched Packets (dropped) = 0, Re-classified packets (redirected) = 0

Configuration sources associated with this session:
Service: DEFAULT, Active Time = 01:00:22
Service: PBHK, Active Time = 01:00:22
Interface: Virtual-Template1, Active Time = 01:00:22
```

Note Portbundle Hostkey and Traffic class cannot be configured under the same policy group.

Step 3 Enter the **show subscriber service** command to find specific information about services on the ISG:

```
Router# show subscriber service example_network_service

  Service "example_network_service":
    Version 1:
      SVM ID                : F1000057
      Child ID              : 54000058
      Locked by             : SVM-Printer            [1]
      Locked by             : PM-Service             [1]
      Locked by             : PM-Info                [1]
      Locked by             : FM-Bind                [1]
      Locked by             : TC-Child               [1]
      Profile               : 65A79818
        Profile name: example_network_service, 3 references
          username             "example_network_service"
          password              apasswd
          traffic-class        "input default drop"
          traffic-class        "output default drop"
          traffic-class        "output access-group 111 priority 10"
          traffic-class        "input access-group 110 priority 10"
          Feature               : TC
          Feature IDB type      : Sub-if or not required
          Feature Data          : 32 bytes:
                                : 000000 00 00 54 00 00 58 00 00  ..t..x..
                                : 000008 00 00 00 00 00 0A 01 00  ........
                                : 000010 00 00 63 B7 6F 08 00 00  ..c.o...
                                : 000018 00 0A 01 00 00 00 63 B7  ......c.
      Version 1:
        SVM ID               : 54000058
        Parent ID            : F1000057
        Locked by            : SVM-Printer            [1]
        Locked by            : FM-Bind                [1]
        Locked by            : TC-Parent              [1]
```

Configuring ISG and SESM Interoperability

The SESM in SSG topologies is configured to use SSO to verify that a subscriber has already been authenticated, and to use PBHK as a session identifier between the SESM and the SSG. Therefore, connecting to the SESM service selection web page from the CPE side will no longer be possible because the ISG has not yet been configured with PBHK. Additionally, the SESM parameters (shared key, ports, IP address of the SESM service selection web page, and so on) need to be added to the ISG. The following steps will restore SESM interoperability with the ISG.

Step 1 Use the **aaa server radius sesm** command to enable a limited-feature RADIUS server and begin adding the SESM parameters to the ISG configuration. This command starts config-locsvr-sesm-radius mode, which accepts parameter settings for the SESM. The following configuration allows the exchange of RADIUS protocol messages between the SESM and the ISG, and restores the RPC channel between the ISG and SESM, together with the SSO functionality.

```
Router# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# aaa server radius sesm
Router(config-locsvr-sesm-radius)# client 10.0.0.1     /* can also use client name
Router(config-locsvr-sesm-radius)# key cisco
Router(config-locsvr-sesm-radius)# port 1812          /* default is port 1645
Router(config-locsvr-sesm-radius)# message-authenticator ignore
```

Step 2 Configure the PBHK in a new service policy map. The following configuration shows the commands to do this.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# policy-map type service ip_portbundle_service
Router(config-service-policymap)# ip portbundle
Router(config-service-policymap)# exit
```

Tip Although it is possible to do so, do not configure the PBHK feature within a *previously* configured service policy map. Use a separate service, for these reasons: Placing a feature under an existing service policy map will trigger that feature only on the flow defined in that traffic class, and not on all traffic of the session. Also, if a feature may need to be disconnected, grouping features makes it necessary to disconnect *all* the features configured in the service policy map. It is not possible to disconnect just one service.

Step 3 The new service policy map gets inserted into the policy control map you associated with the PPPoE session. Enter the following commands to trigger the PBHK feature service directly when the session is started.

Tip Do not overwrite any previous action set in the policy control map. Be sure to increment the action number by 1.

```
Router(config)# policy-map type control example-map2
Router(config-control-policymap)# class type control always event session-start
Router(config-control-policymap-class-control)# 2 service-policy type service name
ip_portbundle_service
Router(config-control-policymap-class-control)# exit
Router(config-control-policymap)# exit
```

Step 4 Configure the PBHK feature to match the settings applied on the SESM by entering the **match** command in config-portbundle mode. In the following configuration commands, the ISG uses its loopback IP address for the PBHK feature (so that whenever a web browser is opened on the client side, the ISG will translate this TCP stream using its loopback IP address as the source IP address rather than the source IP address of the client CPE), and the PBHK feature is used only when the destination of the packet is destined for the default network.

```
Router(config)# ip portbundle
Router(config-portbundle)# source loopback 0
Router(config-portbundle)# ?
IP Portbundle configuration commands:
  default  Set a command to its defaults
  exit     Exit from portbundle configuration mode
  length   Portbundle length configuration
  match    Portbundle match configuration
  no       Negate a command or set its defaults
  source   Portbundle source configuration
```

```
Router(config-portbundle)# match access-list 110
Router(config-portbundle)# exit
```

Step 5 Configure the egress (or *outside*, toward SESM) interface to install the PBHK feature using the following configuration commands. Once this has been done, the interface will do the translation of the source IP address from its origin to the interface configured in config-portbundle configuration mode.

```
Router(config)# interface fa 0/0
Router(config-if)# ip portbundle outside
Router(config-if)# exit
```

Tip Use the **show ip route** command with the IP address of the SESM service selection web page if you need to verify this interface.

See the "CSCuk56681—ISG Sending Locally Defined Service to Portal Breaks Status Page" section on page 89 for additional information about restoring ISG and SESM interoperability.

Verifying ISG and SESM Interaction

Verify that SESM can interact correctly with the ISG after the configuration changes by performing the steps in this section.

Step 1 Bring up a web browser on a PC, then bring up the PPPoE session after reconnecting to the PPPoE session again to register the changes.

Step 2 Direct the web browser to the IP address of the SESM service selection web page and verify that the page displays.

Step 3 Enable the **debug radius** command on the ISG to verify that SSO works correctly. Use reports in the debug output to verify the RADIUS packets exchanged between the SESM and the ISG, as follows:

- The SESM sends access request messages, which contain subattribute 252 ssg-command-info.
- The ISG sends access accept messages with answers to the command request embedded in the ssg-command-info value.

The packet exchange-call flow for communication between ISG and SESM is the same as the communication path between the SSG and the SESM.

Step 4 Enter the **show ip portbundle** command to verify that the PBHK was successfully installed on the session by determining that a bundle was assigned for the session, as follows:

```
Router# show ip portbundle status inuse

Bundle-group 10.10.10.3 has the following in-use port-bundles:-

Port-bundle      VRF Name

64                Default Table

Router# show ip portbundle ip 10.10.10.3 bundle 64

Portbundle IP address: 10.10.10.3  Bundlenumber: 64

Subscriber Portmappings:
Subscriber IP: 10.10.3.1      Subscriber Port: 33487       Mapped Port: 1216
Subscriber IP: 10.10.3.1      Subscriber Port: 33488       Mapped Port: 1217
```

Tip If the **show** command output is empty initially, reload or open the web browser to the SESM service selection web page again.

Configuring Layer 4 Redirect

The SSG is configured to redirect all TCP traffic on port 8090 in SESM, because traffic was classified as having access to an unauthorized service. By completing the steps in this section, the L4 redirection functionality seen on the SSG will be restored on the ISG.

Additional information about redirection can be found in the "Configuring Advertisement and Initial Redirection" section on page 39.

Step 1 Define a new service for the redirection feature and establish when you want to redirect traffic in the policy manager using the following commands. As with the SSG, you want to start redirecting traffic as soon as the PPPoE session is started. This action is defined under the policy control map, as shown in the following commands.

Tip Do not overwrite any previous action set in the policy control map. Be sure to increment the action number by 1.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# policy-map type control example-map2
Router(config-control-policymap)# class type control always event session-start
Router(config-control-policymap-class-control)# 3 service-policy type service name
l4_redirect_service
Router(config-control-policymap-class-control)# exit
Router(config-control-policymap)# exit
```

Step 2 Once you have configured the policy control map, you must implement the service policy map using the following commands. It is here that you will identify which traffic belonging to the session must be redirected using the traffic classification feature.

```
Router(config)# class-map type traffic match-any l4-redirect-tc-map
Router(config-traffic-classmap)# match access-group in name redirect-acl
Router(config-traffic-classmap)# match access-group out name redirect-acl
Router(config-traffic-classmap)# exit
Router(config)# ip access-list extended redirect-acl
Router(config-ext-nacl)# permit tcp any any eq www
Router(config-ext-nacl)# exit
Router(config)# access-list 199 deny tcp any host 10.0.0.1 eq www
Router(config)# access-list 199 deny tcp any host 10.0.0.1 eq 8080
Router(config)# access-list 199 deny tcp host 10.0.0.1 any
Router(config)# access-list 199 permit tcp any any eq www

Router(config)# policy-map type service l4_redirect_service
Router(config-service-policymap)# 10 class type traffic l4-redirect-tc-map
Router(config-service-policymap-class-traffic)# redirect list 199 to group
redirect-group-default
Router(config-service-policymap-class-traffic)# exit
Router(config-service-policymap)# exit
```

The number 10 in the **class type traffic** command sets a priority on the traffic classification feature.

Step 3 To complete the configuration, configure the redirection group by entering the following commands:

```
Router(config)# redirect server-group redirect-group-default
Router(config-sg-l4redirect-group)# server ip 10.0.0.1 port 8090
Router(config-sg-l4redirect-group)# exit
```

Verifying L4 Redirect

Verify that the ISG is correctly configured to redirect all TCP traffic again using L4 Redirect by performing the steps in this section.

Step 1 Bring up a web browser on a PC, then bring up the PPPoE session after reconnecting to the PPPoE session again to register the changes.

Step 2 Direct the web browser to the IP address for the web service. The TCP stream should be redirected to the SESM service selection web page, and the redirection URL should resemble the following pattern:

```
http://10.0.0.1:8080/home?CPURL=http%3A%2F%2F10.0.0.11%2F&t=e42tvk85
```

Step 3 On the ISG router, verify the TCP streams that have been redirected by using the **show redirect translations** command, as follows:

```
Router# show redirect translations

Destination IP/port    Server IP/port         Prot  In Flags  Out Flags  Timestamp
10.0.0.11      80     10.0.0.1         8090   TCP   FIN       FIN        Jan 18 2005
10:33:24
10.0.0.11      80     10.0.0.1         8090   TCP   FIN       FIN        Jan 18 2005
10:33:28
```

The translation data is available only for a short time. You will need to collect this information immediately after entering the IP address in the web browser. Following is an example of the message you receive if you wait too long:

```
Router# show redirect translations
No translations currently exist
```

Step 4 Verify the server group by using the **show redirect group** command, as follows:

```
Router# show redirect group redirect-group-default

Showing all servers of the group redirect-group-default
Server created : using cli
Server           Port
10.30.81.22      8090
```

Step 5 Use the **show subscriber session all** command to check the profile configuration:

```
Router# show subscriber session all

Current Subscriber Information: Total sessions 1
-------------------------------------------------
Unique Session ID: 171
Identifier:
SIP subscriber access type(s): Traffic-Class
Current SIP options: None
Session Up-time: 00:01:21, Last Changed: 00:01:21
AAA unique ID: 0

Session inbound features:
 Feature: Layer 4 Redirect
```

```
  Rule Cfg Definition
  #1 ....
Configuration sources associated with this session:
Service: l4redirect, Active Time = 00:01:21
.
.
.
Policy information:
  Context 6551F5A4: Handle 3E00022D
  Authentication status: authen
  User profile, excluding services:
    ssg-account-info "NSR0600"
    ssg-account-info "NSR0601"
    service-name "SR0600"
    service-name "SR0601"
  Active services associated with session:
    name "service_default_network"
    name "l4redirect"
    name "ip_portbundle"
  Prepaid context: not present
.
.
.
```

Configuring Pass-Through and Proxy Services in a RADIUS Profile

The procedures in this section show you how to configure pass-through and proxy services. For the ISG, a service is defined as a feature, and features can be stored in a RADIUS profile using Cisco AV pairs. However, there is a format change for service profile definitions for the ISG: It no longer interprets the cryptic style used in Cisco's VSA value 251 (Service-Info) profile definitions. Therefore, part of the migration effort for service profiles is to construct similar functionality for a particular SSG service using new Cisco AV pairs defined for the ISG.

The new attributes will be inserted into the existing SSG service profile on the RADIUS server, and the resulting profile will have a mix of old SSG and new ISG attributes. The presence of an attribute that neither the SSG nor the ISG can interpret will not impair functionality, however, because they both routers ignore attributes they do not use and just interpret those they do understand.

Note An exception to this is the R attribute: In an SSG service profile, the R attribute defines the service network destination and is essential for the SSG to populate its own routing tables. If there is no match for the destination IP address, the service is dropped. Additionally, absence of the R attribute in a service profile is interpreted by SESM as meaning that the service is not applicable to the gateway (shows up as highlighted or blue on the SESM service selection web page). Therefore, you need to keep the R attribute statements in the service profiles and add statements that provide functionality required by ISG features.

Configuring Pass-Through Service

The SSG functionality of the R string in the Service-Info attribute is closely related to the traffic classification feature with the **drop** command for default traffic. The procedure in the "Configuring a Traffic Drop Policy" section inserted a traffic drop in the service named example_network_service. The

procedure in this section shows you how to configure a traffic class on the pass-through service and define a traffic class ACL to match whatever IP destination was present in the original R string in the RADIUS profile.

Step 1 The following SSG profile attributes configure the pass-through service named groupA-service1 and specify the service address using the R attribute. (The syntax for these commands depends upon the RADIUS server used.)

```
.
.
.
service outbound
authentication groupA-service1 password apasswd
vsa cisco generic 251 string "MC"
vsa cisco generic 251 string "TP"
vsa cisco generic 251 string "IgroupA-service1"
vsa cisco generic 251 string "R10.0.0.11;255.255.255.255"
```

Configure the equivalent functionality in the ISG by adding traffic classes to the profile, as follows:

```
vsa cisco generic 1 string "ip:traffic-class=in access-group 155 priority 1"
vsa cisco generic 1 string "ip:traffic-class=out access-group 156 priority 1"
```

Step 2 On the ISG, you must manually insert the ACL that is referenced in both traffic class statements (the ACL cannot be downloaded dynamically). The ACL must have equivalent functionality to the RADIUS R string attribute. In the input direction, the destination in the R attribute can be re-created using an ACL where the destination IP route is equivalent to the destination IP route in the R attribute. In the output direction, the R attribute is simulated by using an ACL and configuring the source IP address and network mask to be similar to the destination IP route in the R attribute. The following commands accomplish this equivalency:

```
Router(config)# access-list 155 permit any host 10.0.0.11
Router(config)# access-list 156 permit ip host 10.0.0.11 any
```

This completes the required steps for configuring pass-through service.

Configuring Proxy Service

The following SSG profile attributes configure the proxy service named groupA-service2 and specify the service address using the R attribute:

```
.
.
.
description proxy service
service outbound
authentication groupA-service2 password apasswd
vsa cisco generic 251 string "TX"
vsa cisco generic 251 string "IgroupA-service2"
vsa cisco generic 251 string "S10.0.0.10;1812;1813;ww"
vsa cisco generic 251 string "R10.0.0.12;255.255.255.255"
vsa cisco generic 251 string "MC"
```

Note To preserve proxy service functionality in SESM, the service profile must contain the TX attribute.

The proxy service requires not only a traffic class to construct equivalent functionality to the RADIUS R string attribute, but also requires a policy-directive-authenticate statement be inserted to make certain the username and password on the login page of the SESM service selection web page are authenticated using the method list referenced in the statement. The following steps accomplish this functionality.

Step 1 Insert the following attributes in the service profile:

```
vsa cisco generic 1 string "ip:traffic-class=in access-group 156 priority 11"
vsa cisco generic 1 string "ip:traffic-class=out access-group 56 priority 11"
vsa cisco generic 1 string "subscriber:policy-directive=authenticate aaa list proxy-list"
```

Step 2 Because the name proxy-list refers to a method list name, the ISG configuration needs a new authentication method list for login using this name and pointing to a RADIUS server group. The configuration of the RADIUS server group and the RADIUS server must match the SSG settings within the S string present in the ssg-service-info attribute. For the ISG, the commands to do this are as follows:

```
Router(config)# aaa group server radius proxy-list
Router(config-sg-radius)# server 10.0.0.10 auth-port 1812 acct-port 1813
Router(config-sg-radius)# exit
Router(config)# radius-server host 10.0.0.10 auth-port 1812 acct-port 1813 key ww
Router(config)# aaa authentication login proxy-list group proxy-list
```

Step 3 Configure the ACL referenced in the traffic class string. The ACL should include the destination IP address list found in the ssg-service-info R string subattribute.

```
Router(config)# access-list 56 permit host 10.0.0.12
Router(config)# access-list 156 permit ip any host 10.0.0.12
```

This completes the required steps for configuring proxy service.

Adjusting the Policy Control Map

Once you have adjusted the service profiles on the ISG to contain feature functionality that mimics attributes in the SSG RADIUS service profiles, you may want to adjust the policy control map on the ISG so that it can direct the actions the ISG takes when an event for a service start or stop is triggered.

When a service subscriber clicks a service in the SESM service selection web page, that action sends a RADIUS service logon request to the ISG, which is the same way it works on the SSG. But on the ISG, this action is a service-start event in the policy manager. You must, therefore, implement a service-start event in the service policy map associated with the subscriber. Although *not required*, to demonstrate advantages made possible by the granularity of the policy manager, you could define a class map control policy for every service.

Step 1 The following commands show how to configure a granular control class map:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# class-map type control match-any service1-check
Router(config-control-classmap)# match service-name groupA-service1
Router(config-control-classmap)# exit
Router(config)# class-map type control match-all service2-check
Router(config-control-classmap)# match service-name groupA-service2
Router(config-control-classmap)# exit
```

Step 2 Once you have defined the control class map for service1-check and service2-check, insert the condition trigger in the control policy map for the service logon requests on the ISG by using the following commands:

```
Router(config)# policy-map type control example-map2
Router(config-control-policymap)# class type control service1-check event service-start
Router(config-control-policymap-class-control)# 1 service-policy type service identifier
service-name
Router(config-control-policymap-class-control)# exit
Router(config-control-policymap)# class type control service2-check event service-start
Router(config-control-policymap-class-control)# 1 service-policy type service identifier
service-name
Router(config-control-policymap-class-control)# exit
```

This configuration implies that a control class map is required for each service that you define, but by default, the ISG uses the defined service name to identify a service. If you need to overwrite the default behavior, the ISG offers a list of commands to do so. Consider the following:

```
Router(config)# policy-map type control example-map2
Router(config-control-policymap)# class type control always event service-start
Router(config-control-policymap-class-control)# class type always event service-start
service identifier ?
  authenticated-domain      Authenticated domain name
  authenticated-username    Authenticated username
  dnis                      Dial Number Information Service (called party
                            number)
  nas-port                  NAS Port Identifier
  tunnel-name               VPDN Tunnel-Name
  unauthenticated-domain    Unauthenticated domain name
  unauthenticated-username  Unauthenticated username
```

Step 3 Also as an optional step, you can update the policy manager to perform specific actions when a service is being stopped. Consider the following configuration:

```
Router(config)# policy-map type control example-map2
Router(config-control-policymap)# class type control always event service-stop
Router(config-control-policymap-class-control)#1 service-policy type service unapply
identifier service-name
Router(config-control-policymap-class-control)# exit
```

Tip A sequence order must be followed when actions are applied under a service-start policy: Whenever there is a combination of applying and unapplying services, you must enter all unapply commands first, then enter the apply commands. To do otherwise results in the following message: “action unapply cannot be followed by apply in service-start event.”

Action 1 for a service-stop must be an unapply; otherwise, you will receive the following message: “action 1 supports only unapply identifier service-name in service-stop event.”

Verifying Services

Verify that the ISG services are correctly configured by performing the steps in this section.

Step 1 Bring up a web browser on a PC, then bring up the PPPoE session after reconnecting to the PPPoE session again to register the changes.

Step 2 Direct the web browser to the SESM service selection web page.

Step 3 Click the first service (groupA-service1). This should once again allow you access to the web service page. Refresh the web page to see that content is changed.

Tip You can also test services by sending **ping** commands from the MS-DOS prompt to the web server IP address.

Step 4 Stop the service again using the SESM service selection web page.

Step 5 Click the second service (groupA-service2). After submitting login information, you should once again see the web service page. However, if you enter IP address 10.0.0.12 in the URL field of the web browser, the traffic will be redirected to the SESM service selection web page.

You can also verify connectivity by sending **ping** commands from the MS-DOS prompt to the web server IP address.

Configuring Sequential Service Functionality

In an SSG, it is possible to configure services as either concurrent or sequential. In an ISG, you configure similar functionality. You configure the ISG's policy manager so that when one service starts, all other services are disconnected. These actions use a concept of *unapply*.

Configure the policy manager to perform the correct unapply actions, as follows:

```
Router(config)# policy-map type control SEQUENTIAL_RULE_MAP
Router(config-control-policymap)# class type control CONTROL_CLASS_01 event service-start
Router(config-control-policymap-class-control)# 1 service-policy type service unapply name
02
Router(config-control-policymap-class-control)# 2 service-policy type service identifier
service-name
.
.
.
Router(config-control-policymap)# class type control CONTROL_CLASS_02 event service-start
Router(config-control-policymap-class-control)# 1 service-policy type service unapply name
01
Router(config-control-policymap-class-control)# 2 service-policy type service identifier
service-name
.
.
.
Router(config-control-policymap)# class type control always event session-start
Router(config-control-policymap-class-control)# 1 authenticate aaa list CAR
Router(config-control-policymap-class-control)# 2 service-policy type service name PBHK
Router(config-control-policymap-class-control)# 3 service-policy type service name DEFAULT
.
.
.
```

When you activate service 02 with this configuration, the ISG deactivates service 01, and the other way around.

Configuring Prepaid Service

The following SSG attributes configure the prepaid service named groupA-service3 and specify the service address using the R attribute:

```
.
.
.
description SSG to ISG migration example
service outbound
authentication groupA-service3 password apasswd
vsa cisco generic 251 string "MC"
vsa cisco generic 251 string "TP"
vsa cisco generic 251 string "Z"
vsa cisco generic 251 string "IgroupA-service3"
vsa cisco generic 251 string "R10.0.0.13;255.255.255.255"
```

Perform the following steps to configure prepaid service on the ISG:

Step 1 In the ISG, configure functionality equivalence to the RADIUS R string attribute provided in the SSG profile by using traffic classes. See the following example:

```
vsa cisco generic 1 string "ip:traffic-class=in access-group 157 priority 1"
vsa cisco generic 1 string "ip:traffic-class=out access-group 57 priority 1"
```

Step 2 The ACL numbers in the Cisco AV pair must be redefined on the ISG and must match the values configured in the SSG R attribute. Use the **access-list** command, as follows::

```
Router(config)# access-list 57 permit host 10.0.0.13
Router(config)# access-list 157 permit ip any host 10.10.0.13
```

Step 3 The following command shows how to configure the prepaid feature in the RADIUS profile. You must insert a new attribute in the service profile, because the prepaid Z attribute in the SSG is not being interpreted by the ISG anymore.

```
vsa cisco generic 1 string "prepaid-config=default"
```

The name “default” refers to a prepaid server configuration present on the ISG itself, but you will need to insert additional configurations on the ISG to complete the prepaid functionality. These settings are needed to reauthorize packets exchanged between the billing server and the ISG. Compared to the SSG, the ISG offers more specific configurations for prepaid service such as different thresholds, a different billing server group for reauthorization, and so on.

Step 4 Use the **?** command to display the prepaid subcommands:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# subscriber feature prepaid default
Router(config-prepaid)# ?
Prepaid subcommands
  default           Set a command to its defaults
  exit              Exit from subcommand
  interim-interval  Interim interval config
  method-list       Method list config
  no                Negate a command or set its defaults
  password          Password config
  threshold         Threshold config
```

Step 5 In your configuration, you could implement an authorization and accounting method list and password to use for RADIUS reauthorization access requests that are sent to the billing server using the following commands:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# subscriber feature prepaid default
Router(config-prepaid)# method-list authorization default
Router(config-prepaid)# method-list accounting default
Router(config-prepaid)# password apasswd
```

Note Remember that default settings are not listed in the configuration. When you look at the configuration of the ISG after implementing the previous commands, you will not see any of them in the configuration if they are default settings.

Step 6 The following commands are always mandatory in the configuration of both the ISG or SSG, whenever the prepaid feature is deployed. Attribute 55 is a UNIX time stamp and attribute 44 is acct-session-id.

```
Router(config)# radius-server attribute 55 include-in-acct-req
Router(config)# radius-server attribute 44 include-in-access-req
```

Step 7 To complete the configuration, match a specific class control condition when the prepaid service is started or stopped. The following commands extend the control class map created previously with the current service name:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# class-map type control match-any service1-check
Router(config-control-classmap)# match service-name groupA-service3
Router(config-control-classmap)# exit
```

Verifying Prepaid Service

Verify that the ISG prepaid feature functions correctly by performing the steps in this section.

Step 1 Bring up a web browser on a PC, then bring up the PPPoE session after reconnecting to the PPPoE session again to register the changes.

Step 2 Direct your browser to the SESM service selection web page.

Step 3 Click the first service (groupA-service3). The prepaid service should be triggered again.

Step 4 To verify that the service was activated, open a web browser and direct it to the IP address defined in Step 2 of the "Configuring Prepaid Service" procedure:

```
http://10.0.0.13
```

Tip Alternatively, you can source pings from an MS-DOS prompt on the PC to IP address 10.0.0.13.

Step 5 The service can be verified by obtaining the identifier created for the traffic class, and by verifying the service itself by using the **show subscriber service** and **show subscriber session** commands, as follows:

```
Router# show subscriber service groupA-service3

  Service "groupA-service3":
    Version 1:
      SVM ID                : A4000068
      Child ID              : 32000069
      Locked by             : SVM-SIP-Info           [1]
      Locked by             : SVM-Printer            [1]
      Locked by             : PM-Service             [1]
      Locked by             : PM-Info                [1]
      Locked by             : FM-Bind                [1]
      Locked by             : TC-Child               [1]
      Profile               : 65AC5FE8
        Profile name: group3-service3, 4 references
          service-type         5 [Outbound]
          ssg-service-info     "MC"
          ssg-service-info     "TP"
          ssg-service-info     "Z"
          ssg-service-info     "IgroupA-service3"
          ssg-service-info     "R10.0.0.13;255.255.255.255"
          traffic-class        "in access-group 157 priority 1"
          traffic-class        "out access-group 57 priority 1"
          policy-handle        1795162340 (0x6B0000E4)
          Feature               : TC
          Feature IDB type      : Sub-if or not required
          Feature Data          : 32 bytes:
                                : 000000 00 00 32 00 00 69 6B 00  ..2..ik.
                                : 000008 00 E4 00 00 00 01 00 00  ........
                                : 000010 00 00 63 BC 46 EC 00 00  ..c.f...
                                : 000018 00 01 00 00 00 00 63 BC  ......c.
          SIP                   : Info 6475A690 access: PPP info: PPP
      Version 1:
        SVM ID                : 32000069
        Parent ID             : A4000068
        Locked by             : SVM-Printer            [1]
        Locked by             : FM-Bind                [1]
        Locked by             : TC-Parent              [1]

Router# show subscriber session

Current Subscriber Information: Total sessions 1

Uniq ID Interface  State          Service      Identifier           Up-time
56      Traffic-Cl unauthen       Ltm Internal    user-group3 00:00:34
54      Traffic-Cl connected      Ltm Internal    00:00:56
55      Traffic-Cl connected      Ltm Internal    00:00:56
53      Vi2.1      authen         Local Term      user-group3 00:00:56

Router# show subscriber session uid 56

Subscriber session handle: 6E0000E6, state: connected, service: Ltm
Internal
Unique Session ID: 56
Identifier: user-group3
SIP subscriber access type(s): Traffic-Class
Root SIP Handle: 23000026, PID: 98
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:01:04, Last Changed: 00:01:04
AAA unique ID: 0
Switch handle: 1037

Policy information:
```

```
  Context 65A89EE8: Handle 6B0000E4
  Authentication status: unauthen
  Prepaid context: default
    threshold time 0 seconds
    threshold volume 0 bytes
    method-list author default
    method-list accounting default
    password apasswd
    Interim accounting disabled
    State PREPAID_FEATURE_RUNNING
    Flow idle ? NO
    Acct start sent ? YES

Session inbound features:
 Feature: Prepaid Volume Monitor
   Threshold:4294967295 - Quota:4294967295
   Usage(since last update):0 - Total:0
   Current states: Start
Session outbound features:
 Feature: Prepaid Volume Monitor
   Threshold:4294967295 - Quota:4294967295
   Usage(since last update):0 - Total:0
   Current states: Start
Non-datapath features:
 Feature: Time Monitor
   Threshold: 100 (seconds) - Quota: 100 (seconds)
   Session time: 66 (seconds)
Configuration sources associated with this session:
Service: groupA-service3, Active Time = 00:01:06
```

Configuring a Policy Map and Traffic Classifications

The task in this section shows how to configure prioritization based on an ACL, use of the traffic classification feature, L4 redirection, and a prepaid-based service. This section describes:

- How the policy manager works.
- Differences between a policy control map and a service policy.
- Why a feature like Prepaid needs to be configured in a remote service profile.
- How prioritization works in the traffic classification feature.

Policy control is that part in the policy manager that makes certain that specific actions are triggered for specific events. The action itself is most often linked to a policy service. The policy service is responsible for inserting into the subscriber flow features such as PBHK, L4 redirection, prepaid functionality, drop packets, or traffic classification. Therefore, a policy service provides the ISG with the ability to insert policies on the traffic flow.

For the task described in this section, a policy map is implemented on the ISG that:

- Redirects all TCP traffic to IP addresses 10.40.96.4 and 10.40.96.5, as long as the prepaid service has not been activated by an **event session-start** command in a control policy map.
- Allows all IP traffic to address 10.40.96.4 to pass through as soon as the prepaid service named pp-quota-refill-time has been activated by an **event service-start** command in a control policy map.

Step 1 Use the following commands to configure the control policy map such that any subscriber session that is associated with this policy map will have two actions to perform at the time that the session is started on the ISG: Action 1 is to authenticate the session using the AAA method list named ML-1. Action 2 defines a policy service that must be inserted.

```
Router(config)# policy-map type control prepaid-user
Router(config-control-policymap)# class type control always event session-start
Router(config-control-policymap-class-control)# 1 authenticate aaa list ML-1
Router(config-control-policymap-class-control)# 2 service-policy type service name
prepaid-redirect
Router(config-control-policymap-class-control)# exit
Router(config-control-policymap)# class type control always event service-start
Router(config-control-policymap-class-control)# 1 service-policy type service aaa list
ML-1 identifier service-name
Router(config-control-policymap-class-control)# exit
Router(config-control-policymap)# class type control always event quota-depleted
Router(config-control-policymap-class-control)# exit
Router(config-control-policymap)# class type control always event credit-exhausted
Router(config-control-policymap-class-control)# exit
```

Step 2 Once you have configured the policy control map, you must implement the service policy map. The following service policy map combines two features, traffic classification and redirection. Traffic classification ensures that only a specific part of the traffic is redirected, and that the remaining flow is left unchanged. The remaining traffic is filtered out when you define a traffic class map that links the traffic class feature with an extended ACL named prepaid-redirect-acl. The policy service will redirect all TCP traffic at IP addresses 10.40.96.4 and 10.40.96.5 to the SESM service selection web page.

The policy that will be inserted on the traffic flow is the service policy map named prepaid-redirect-tc as defined in the action rule, and is configured as follows:

```
Router(config)# policy-map type service prepaid-redirect
Router(config-service-policymap)# 10 class type traffic prepaid-redirect-tc
Router(config-service-policymap-class-traffic)# redirect to ip 10.30.81.22 port 8090
.
.
.
Router(config)# class-map type traffic match-any prepaid-redirect-tc
Router(config-traffic-classmap)# match access-group output name prepaid-redirect-acl
Router(config-traffic-classmap)# match access-group input name prepaid-redirect-acl
Router(config-traffic-classmap)# exit
Router(config)# ip access-list extended prepaid-redirect-acl
Router(config-ext-nacl)# permit tcp any host 10.40.96.5
Router(config-ext-nacl)# permit tcp any host 10.40.96.4
```

The ISG is forced to redirect all the TCP traffic destined to IP addresses 10.40.96.4 and 10.40.96.5 as soon as the subscriber session comes up. The control policy map links the action with an event, and the service policy map indicates to the ISG what type of policy to apply to the traffic flow.

Step 3 Let us say that the subscriber can start a prepaid service named pp-quota-refill-time as a subsequent event. This event is linked with a service logon request sent from the SESM to the ISG. Again, the control policy map indicates to the ISG what actions to take when a service logon happens on the SESM service selection web page.

To set up this action, insert the following commands in the policy map:

```
Router(config-control-policymap)# class type control always event service-start
Router(config-control-policymap-class-control)# 1 service-policy type service aaa list
ML-1 identifier service-name
```

These commands initiate a search via the AAA method list named ML-1 to determine if there is a RADIUS service profile available on a remote RADIUS server with username service-name (taken from the service logon sent by SESM).

Step 4 The following attributes configure the service that the subscriber selects on the RADIUS server. The attributes that are interpreted only by the ISG are shown in bold text for purpose of example.

```
.
.
.
service outbound
authentication prepaid-volume password servicecisco
vsa cisco generic 251 string "MC"
vsa cisco generic 251 string "TP"
vsa cisco generic 251 string "I"pp-quota-refill-time"
vsa cisco generic 251 string "Z"
vsa cisco generic 1 string "prepaid-config=default"
vsa cisco generic 251 string "R10.40.96.4;255.255.255.255"
vsa cisco generic 1 string "ip:traffic-class=in access-group name pp-quota-refill-time
priority 5"
vsa cisco generic 1 string "ip:traffic-class=out access-group name pp-quota-refill-time
priority 5"
```

Step 5 A prepaid service is always defined in combination with a traffic class. In this configuration, the policy service is not configured locally but remotely on the RADIUS server. The traffic flow on which this policy service will work is based on the extended ACL group named pp-quota-refill-time, which is configured as follows:

```
Router(config)# ip access-list extended pp-quota-refill-time
Router(config-ext-nacl)# permit ip any host 10.40.96.4
Router(config-ext-nacl)# permit ip host 10.40.96.4 any
```

Notice that the redirection service that is triggered first at session start was not unapplied, and that there is an ACL that overlaps with the redirection list. When a TCP connection to IP address 10.40.96.4 is opened, the connection will work because of the prioritization possible in the traffic class feature. The presence of the number 10 in the **10 class type traffic prepaid-redirect-tc** command on the service policy for redirection, and priority 5 in the **vsa cisco generic 1 string "ip:traffic-class=in access-group name pp-quota-refill-time priority 5"** command, make certain that the ISG tries first to match any traffic in the flow against the ACL for the service, and then other ACLs with a lower priority. As such, TCP traffic for IP address 10.40.96.5 will match on the ACL defined in the prepaid service and will not be redirected.

This configuration shows that a policy service need not always be configured locally. You can insert a service policy remotely on a RADIUS server. Remember that ACLs must be present on the ISG before you set policy on a RADIUS server, and that a control policy map cannot be configured remotely on a RADIUS server.

The service policy is simply a traffic class on which no special action such as L4 redirection or traffic drop are taken on the traffic. The configuration allows traffic to IP address 10.40.96.4 to pass through without any alteration.

Configuring Advertisement and Initial Redirection

Using advertisement redirection (RA) and initial redirection (RI) features (defined using the SSG RADIUS RI and RA attribute) do not work on the ISG (see CSCsa63459 for more information). The following steps will replace the functionality provided by the SSG RADIUS RI and RA attributes on the ISG. Other services will not be impacted by this configuration.

Step 1 Configure the local service on the ISG. In this example, the service is named l4redirect:

```
Router(config)# policy-map type service l4redirect
Router(config-service-policymap)# class type traffic CLASS-ALL
Router(config-service-policymap-class-traffic)# redirect list 160 to ip 10.40.100.3 port
80 duration 20
Router(config-service-policymap-class-traffic)# redirect list 163 to ip 10.40.101.3 port
80 duration 10 frequency 60
Router(config-service-policymap-class-traffic)# exit

Router(config)# policy-map type control control_default_network
Router(config-control-policymap)# class type control always event session-start
Router(config-control-policymap-class-control)# 1 authenticate aaa list SESM
Router(config-control-policymap-class-control)# 2 service-policy type service name
ip_portbundle
Router(config-control-policymap-class-control)# 3 service-policy type service name
service_default_network
Router(config-control-policymap-class-control)# 4 service-policy type service name
l4redirect
Router(config-control-policymap-class-control)# exit

Router(config-control-policymap)# class type control always event service-start
Router(config-control-policymap-class-control)# 1 service-policy type service identifier
service-name
Router(config-control-policymap-class-control)# exit
Router(config-control-policymap)# class type control always event service-stop
Router(config-control-policymap-class-control)# 1 service-policy type service unapply
identifier service-name
```

Step 2 Configure ACLs that match the service to be redirected. In this example, a service provides access to IP network 10.40.96.0 and another service goes to IP network 10.40.97.0:

```
Router(config)# access-list 160 permit ip any 10.40.96.0 0.0.0.255
Router(config)# access-list 163 permit ip any 10.40.97.0 0.0.0.255
```

At session start, the service named l4redirect is started and packets that match the source address for ACL 160 are redirected to IP address 10.40.100.3 (an advertisement server) for 20 seconds; see the first **redirect list** command in Step 1. This configuration replaces advertisement redirection.

The same configuration is specified for advertisement redirection. The redirect list function polls for packets to redirect every 60 seconds for 10 seconds. Packets that match the source address for ACL 163 are redirected to IP address 10.40.101.3; see the second **redirect list** command in Step 1. This configuration replaces initial redirection.

Configuring L2 Service Selection

On the SSG, a subscriber using PPP typically initiates a Layer 2 (L2) session using a desktop PPP dialer and specifying either a structured or nonstructured username and password. (On the CPE side of the network, an always-on model is often adopted, and often with a preconfigured username and password.)

A structured username contains a username and the domain or service name. An example is user1@service.net. An unstructured username contains the username without the domain and service name specified— the name user1 by itself is an example of an unstructured username. User1 in this example could access multiple services simultaneously from a single PPP session.

A structured username can serve to authenticate a subscriber and as a service selection method. As a part of the Account Logon feature, the username is used to authenticate subscriber access to the SSG. The service part of the structured username is used by the Service Logon feature to select the specified service. As long as the PPP session is terminated and not forwarded to the home gateway or Layer 2 network server (LNS), subscribers with a structured username can also connect to the SESM service selection web page and use their web browser to select services.

The nonstructured username specifies only the username, and is used by the Account Logon feature on the SSG to authenticate subscriber access. Subscribers with a nonstructured username must use their browser to connect to the SESM Dashboard Server and then log on to different services.

To implement the same structured username functionality on the ISG as on the SSG, you need to add an action in a policy map that downloads the service profile from a AAA server (which is specified by the **aaa method-list** command) based on the unauthenticated domain name.

To add this action to a policy map, define a policy map and enter the following commands to implement L2 service selection on the ISG:

```
Router(config)# policy-map type control DEFAULT_RULE_MAP
Router(config-control-policymap)# class type control always event session-start
Router(config-control-policymap-class-control)# 1 authenticate aaa list CAR
Router(config-control-policymap-class-control)# 2 service-policy type service name PBHK
Router(config-control-policymap-class-control)# 3 service-policy type service name DEFAULT
Router(config-control-policymap-class-control)# 4 service-policy type service aaa list CAR
identifier unauthenticated-domain
```

The action must be applied after the action that authenticates the subscriber. In the previous commands, this action would occur after action 1.

Verifying L2 Service Selection

Verify that the ISG is correctly configured to implement L2 service selection by performing the steps in this section.

Step 1 Configure a PPP user with username U0019@SR0013.

Step 2 Use the **show subscriber session username** command to verify that the service is activated when the user logs in, as follows:

```
Router# show subscriber session username U0019@SR0013

Unique Session ID: 521
Identifier: U0019@SR0013
SIP subscriber access type(s): PPPoA/PPP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:00:13, Last Changed: 00:00:13
AAA unique ID: 336
Interface: Virtual-Access4

Policy information:
  Context 2078F3B0: Handle A50003C7
  Authentication status: authen
  Active services associated with session:
    name "SR0013"
    name "DEFAULT"
```

```
    name "PBHK"
  Rules, actions and conditions executed:
    subscriber rule-map DEFAULT_RULE_MAP
      condition always event session-start
        1 authenticate aaa list CAR
        2 service-policy type service name PBHK
        3 service-policy type service name DEFAULT
        4 service-policy type service aaa list CAR identifier unauthenticated-domain

Session inbound features:
Traffic classes:
  Traffic class session ID: 522
   ACL Name: DEFAULT_IACL, Packets = 0, Bytes = 0
  Traffic class session ID: 523
   ACL Name: SR0013_IACL, Packets = 0, Bytes = 0
 Default traffic is dropped
 Unmatched Packets (dropped) = 0, Re-classified packets (redirected) = 0

 Feature: Portbundle Hostkey
 Portbundle IP = 10.10.100.7     Bundle Number = 162

Session outbound features:
Traffic classes:
  Traffic class session ID: 522
   ACL Name: DEFAULT_OACL, Packets = 0, Bytes = 0
  Traffic class session ID: 523
   ACL Name: SR0013_OACL, Packets = 0, Bytes = 0
 Default traffic is dropped
 Unmatched Packets (dropped) = 0, Re-classified packets (redirected) = 0

Configuration sources associated with this session:
Service: SR0013, Active Time = 00:00:14
Service: DEFAULT, Active Time = 00:00:14
Service: PBHK, Active Time = 00:00:14
Interface: Virtual-Template1, Active Time = 00:00:14
```

Step 3 Use the **show subscriber service** command to display specific information about services on the ISG, as follows:

```
Router# show subscriber service SR0013

  Service "SR0013":
    Version 1:
      SVM ID               : 54000151
      Child ID             : D8000152
      Locked by            : SVM-Printer            [1]
      Locked by            : PM-Service             [1]
      Locked by            : PM-Info                [1]
      Locked by            : FM-Bind                [1]
      Locked by            : TC-Child               [1]
      Profile              : 64B2F0B0
        Profile name: SR0013, 3 references
          traffic-class        "in access-group name SR0013_IACL priority 1"
          traffic-class        "out access-group name SR0013_OACL priority 1"
          ssg-service-info     "ISR0013 (L2 service selection)"
          ssg-service-info     "R10.40.96.32;255.255.255.255"
          ssg-service-info     "TP"
          ssg-service-info     "MC"
      Feature              : TC
          Feature IDB type      : Sub-if or not required
          Feature Data          : 28 bytes:
                                : 000000 00 00 D8 00 01 52 00 00  .....r..
                                : 000008 00 01 00 00 00 00 64 B8  ......d.
                                : 000010 B0 E8 00 00 00 01 00 00  ........
```

```
                          : 000018 00 00 20 AE              .. .
Version 1:
  SVM ID                : D8000152
  Parent ID             : 54000151
  Locked by             : SVM-Printer            [1]
  Locked by             : FM-Bind                [1]
  Locked by             : TC-Parent              [1]
```

Special Note about Configuring a PTA-MD Exclusion List

On the SSG, L2 service selection is the default behavior. If you want to override this behavior, you use the PPP Termination and Aggregation Multi-Domain (PTA-MD) exclusion feature to configure an exclusion list specifying every domain for which you want to disable L2 service selection, either remotely or locally.

The following commands are used for this configuration:

```
Router(config)# ssg multidomain ppp
Router(config-auto-domain)# download exclude-profile profile-name password
Router(config-auto-domain)# download exclude-profile remote-exclude-profile password
Router(config-auto-domain)# exclude domain realm> local-exclude-profile
```

A remote exclude profile is downloaded from a AAA server and includes the Control-Info XP attribute for specifying which realm you want to exclude, as follows:

```
Cisco-SSG-control-info="XPrealm"
```

Because there is no equivalent **ssg multidomain ppp** command on the ISG, the ISG cannot download remote exclude profiles. Therefore, the XP attribute is meaningless to the ISG.

In the case of local exclude profiles on the ISG, you cannot exclude domains on an individual basis. The configuration as described in "Configuring L2 Service Selection" section on page 39 parses every structured username (user@domain or user@service) in the same manner, regardless of the domain or service name. This is because the configuration to make L2 service selection work requires use of an always condition in the control class within the event session-start. The following commands show this configuration:

```
Router(config)# policy-map type control DEFAULT_RULE_MAP
Router(config-control-policymap)# class type control always event session-start
Router(config-control-policymap-class-control)# 1 authenticate aaa list CAR
Router(config-control-policymap-class-control)# 2 service-policy type service name PBHK
Router(config-control-policymap-class-control)# 3 service-policy type service name DEFAULT
Router(config-control-policymap-class-control)# 4 service-policy type service aaa list CAR
identifier unauthenticated-domain
```

No other event on the ISG, apart from session start, can be selected to make it possible to include a control condition on an event to only allow certain service names to trigger a RADIUS request, as is done by the PTA-MD exclusion feature on SSG.

SSG and ISG Accounting and RADIUS Update Examples

RADIUS accounting packets are counted differently on the ISG than they are on the SSG. Also, ISG input packets are seen on the SSG as output packets. Use the information in the following sections to understand and correct these differences:

SSG AAA Accounting

In the SSG, the following command enables AAA accounting of services for billing with a RADIUS server:

```
aaa accounting network SESM start-stop group SESM
```

The following attributes are defined in the SSG RADIUS profile:

```
Acct-Interim-Interval = 60
Cisco-AVpair = subscriber:accounting-list=SESM
```

Note These commands and attributes enable accounting updates for the user in PPP sessions only, and not for the services.

The following example shows a log of accounting activity on the SSG, including session start (see bold text):

```
Apr  5 08:36:31.838: RADIUS/ENCODE(0000000D):Orig. component type = PPoA
Apr  5 08:36:31.838: RADIUS(0000000D): Storing nasport 0 in rad_db
Apr  5 08:36:31.838: RADIUS(0000000D): Config NAS IP: 0.0.0.0
Apr  5 08:36:31.838: RADIUS(0000000D): sending
Apr  5 08:36:31.838: RADIUS/ENCODE: Best Local IP-Address 10.10.67.2 for Radius-Server
10.30.81.30
Apr  5 08:36:31.838: RADIUS(0000000D): Send Accounting-Request to 10.30.81.30:1813 id
1646/166, len 141
Apr  5 08:36:31.838: RADIUS:  authenticator E2 FC 2D BB FC 1F C8 B7 - D3 7F F4 E0 CF 77 58
E2
Apr  5 08:36:31.838: RADIUS:  Acct-Session-Id     [44]  10  "00000139"
Apr  5 08:36:31.838: RADIUS:  Vendor, Cisco       [26]  32
Apr  5 08:36:31.838: RADIUS:   Cisco AVpair       [1]   26  "connect-progress=Call Up"
Apr  5 08:36:31.838: RADIUS:  Vendor, Cisco       [26]  24
Apr  5 08:36:31.838: RADIUS:   ssg-account-info   [250] 18  "S10.10.100.11:64"
Apr  5 08:36:31.838: RADIUS:  Acct-Authentic      [45]  6   RADIUS                    [1]
Apr  5 08:36:31.838: RADIUS:  Acct-Status-Type    [40]  6   Start                    [1]
Apr  5 08:36:31.838: RADIUS:  NAS-Port-Type       [61]  6   Virtual                  [5]
Apr  5 08:36:31.838: RADIUS:  NAS-Port            [5]   6   0
Apr  5 08:36:31.838: RADIUS:  NAS-Port-Id         [87]  13  "5/0/0/1.300"
Apr  5 08:36:31.838: RADIUS:  Service-Type        [6]   6   Framed                   [2]
Apr  5 08:36:31.838: RADIUS:  NAS-IP-Address      [4]   6   10.10.67.2
Apr  5 08:36:31.838: RADIUS:  Acct-Delay-Time     [41]  6   0
Apr  5 08:36:31.930: RADIUS: Received from id 1646/166 10.30.81.30:1813,
Accounting-response, len 20
Apr  5 08:36:31.930: RADIUS:  authenticator 99 7F C3 F4 B3 39 39 C7 - 02 0A EE 6A A5 61 B7
0E
```

The following example shows a log of accounting activity on the SSG, including watchdog activity (see bold text):

```
Apr  5 08:41:02.210: RADIUS/ENCODE(0000001C):Orig. component type = SSG
Apr  5 08:41:02.210: RADIUS(0000001C): Using existing nas_port 0
Apr  5 08:41:02.210: RADIUS(0000001C): Config NAS IP: 0.0.0.0
Apr  5 08:41:02.210: RADIUS(0000001C): sending
```

```
Apr  5 08:41:02.210: RADIUS/ENCODE: Best Local IP-Address 10.10.67.2 for Radius-Server
10.30.81.30
Apr  5 08:41:02.210: RADIUS(0000001C): Send Accounting-Request to 10.30.81.30:1813 id
1646/170, len 222
Apr  5 08:41:02.210: RADIUS:  authenticator 7B 3F FE 09 FC 91 B6 E6 - 16 A5 74 BE DA 77 03
44
Apr  5 08:41:02.210: RADIUS:  Acct-Session-Id     [44]  10  "000001C2"
Apr  5 08:41:02.210: RADIUS:  Framed-IP-Address   [8]   6   10.20.81.1
Apr  5 08:41:02.210: RADIUS:  Framed-Protocol     [7]   6   PPP                         [1]
Apr  5 08:41:02.210: RADIUS:  User-Name           [1]   7   "U0509"
Apr  5 08:41:02.210: RADIUS:  Vendor, Cisco       [26]  32
Apr  5 08:41:02.210: RADIUS:   Cisco AVpair       [1]   26  "connect-progress=Call Up"
Apr  5 08:41:02.210: RADIUS:  Vendor, Cisco       [26]  24
Apr  5 08:41:02.210: RADIUS:   ssg-account-info   [250] 18  "S10.10.100.11:64"
Apr  5 08:41:02.210: RADIUS:  Vendor, Cisco       [26]  16
Apr  5 08:41:02.210: RADIUS:   ssg-control-info   [253] 10  "I0;15699"
Apr  5 08:41:02.210: RADIUS:  Vendor, Cisco       [26]  16
Apr  5 08:41:02.210: RADIUS:   ssg-control-info   [253] 10  "O0;19471"
Apr  5 08:41:02.210: RADIUS:  Acct-Session-Time   [46]  6   116
Apr  5 08:41:02.210: RADIUS:  Acct-Input-Octets   [42]  6   0
Apr  5 08:41:02.210: RADIUS:  Acct-Output-Octets  [43]  6   0
Apr  5 08:41:02.210: RADIUS:  Acct-Input-Packets  [47]  6   0
Apr  5 08:41:02.210: RADIUS:  Acct-Output-Packets [48]  6   0
Apr  5 08:41:02.214: RADIUS:  Acct-Authentic      [45]  6   RADIUS                      [1]
Apr  5 08:41:02.214: RADIUS:  Acct-Status-Type    [40]  6   Watchdog                   [3]
Apr  5 08:41:02.214: RADIUS:  NAS-Port-Type       [61]  6   Virtual                    [5]
Apr  5 08:41:02.214: RADIUS:  NAS-Port            [5]   6   0
Apr  5 08:41:02.214: RADIUS:  NAS-Port-Id         [87]  13  "5/0/0/1.300"
Apr  5 08:41:02.214: RADIUS:  Service-Type        [6]   6   Framed                     [2]
Apr  5 08:41:02.214: RADIUS:  NAS-IP-Address      [4]   6   10.10.67.2
Apr  5 08:41:02.214: RADIUS:  Acct-Delay-Time     [41]  6   0
Apr  5 08:41:02.274: RADIUS: Received from id 1646/170 10.30.81.30:1813,
Accounting-response, len 20
Apr  5 08:41:02.274: RADIUS:  authenticator B9 9A 96 29 2D AB EF 0D - 33 61 3D E4 26 95 F7
A0
```

The following example shows a log of accounting activity on the SSG, including session stop (see bold text):

```
Apr  5 08:42:02.198: RADIUS/ENCODE(0000001C):Orig. component type = SSG
Apr  5 08:42:02.198: RADIUS(0000001C): Using existing nas_port 0
Apr  5 08:42:02.198: RADIUS(0000001C): Config NAS IP: 0.0.0.0
Apr  5 08:42:02.198: RADIUS(0000001C): sending
Apr  5 08:42:02.198: RADIUS/ENCODE: Best Local IP-Address 10.10.67.2 for Radius-Server
10.30.81.30
Apr  5 08:42:02.198: RADIUS(0000001C): Send Accounting-Request to 10.30.81.30:1813 id
1646/171, len 264
Apr  5 08:42:02.198: RADIUS:  authenticator 55 B7 F7 DE F1 63 5C DA - 00 CE 69 ED 22 76 7D
55
Apr  5 08:42:02.198: RADIUS:  Acct-Session-Id     [44]  10  "000001C2"
Apr  5 08:42:02.198: RADIUS:  Framed-IP-Address   [8]   6   10.20.81.1
Apr  5 08:42:02.198: RADIUS:  Framed-Protocol     [7]   6   PPP                         [1]
Apr  5 08:42:02.198: RADIUS:  User-Name           [1]   7   "U0509"
Apr  5 08:42:02.198: RADIUS:  Acct-Authentic      [45]  6   RADIUS                      [1]
Apr  5 08:42:02.198: RADIUS:  Vendor, Cisco       [26]  32
Apr  5 08:42:02.202: RADIUS:   Cisco AVpair       [1]   26  "connect-progress=Call Up"
Apr  5 08:42:02.202: RADIUS:  Vendor, Cisco       [26]  24
Apr  5 08:42:02.202: RADIUS:   ssg-account-info   [250] 18  "S10.10.100.11:64"
Apr  5 08:42:02.202: RADIUS:  Vendor, Cisco       [26]  16
Apr  5 08:42:02.202: RADIUS:   ssg-control-info   [253] 10  "I0;15699"
Apr  5 08:42:02.202: RADIUS:  Vendor, Cisco       [26]  16
Apr  5 08:42:02.202: RADIUS:   ssg-control-info   [253] 10  "O0;19471"
Apr  5 08:42:02.202: RADIUS:  Acct-Session-Time   [46]  6   176
Apr  5 08:42:02.202: RADIUS:  Acct-Input-Octets   [42]  6   0
```

```
Apr  5 08:42:02.202: RADIUS:  Acct-Output-Octets  [43]  6   0
Apr  5 08:42:02.202: RADIUS:  Acct-Input-Packets  [47]  6   0
Apr  5 08:42:02.202: RADIUS:  Acct-Output-Packets [48]  6   0
Apr  5 08:42:02.202: RADIUS:  Acct-Terminate-Cause[49]  6   user-request              [1]
Apr  5 08:42:02.202: RADIUS:  Vendor, Cisco       [26]  36
Apr  5 08:42:02.202: RADIUS:   Cisco AVpair       [1]   30  "disc-cause-ext=No Disconnect"
Apr  5 08:42:02.202: RADIUS:  Acct-Status-Type    [40]  6   Stop                      [2]
Apr  5 08:42:02.202: RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
Apr  5 08:42:02.202: RADIUS:  NAS-Port            [5]   6   0
Apr  5 08:42:02.202: RADIUS:  NAS-Port-Id         [87]  13  "5/0/0/1.300"
Apr  5 08:42:02.202: RADIUS:  Service-Type        [6]   6   Framed                    [2]
Apr  5 08:42:02.202: RADIUS:  NAS-IP-Address      [4]   6   10.10.67.2
Apr  5 08:42:02.202: RADIUS:  Acct-Delay-Time     [41]  6   0
Apr  5 08:42:02.254: RADIUS: Received from id 1646/171 10.30.81.30:1813,
Accounting-response, len 20
Apr  5 08:42:02.254: RADIUS:  authenticator 3B ED BC B8 52 E3 36 3F - 52 CC 4E 44 0F C7 AD
0C
```

SSG Accounting Configuration Alternatives

You can also enable accounting without using the **aaa accounting network SESM start-stop group SESM** command, and instead use the **ssg accounting per-host** command. This command provides start and stop updates for user login and logout, but not for the services. To enable accounting start and stop updates for the services you would use the **ssg accounting per-service** command. No updates are sent for user login and logout with this command.

Note Only one of the **ssg accounting commands**, either **ssg accounting per-host** or **ssg accounting per-service**, can be configured at one time. Configuring one command disables the other.

Another way to enable accounting on the SSG is by using the **ssg accounting interval 60** command, which causes updates for user login and logout, service enable and disable, and regular updates every 60 seconds.

You can fine-tune the **ssg accounting interval 60** command by configuring specific services using the Service-Info L attribute. The L attribute overwrites the local configuration and provides a way to disable accounting updates for a specific service. The following attribute:

```
cisco-SSG-service-info = L0;disable
```

disables the accounting updates for a service. There is no way to configure the accounting update rate for the user using RADIUS attributes.

The following example shows a log of accounting activity on the SSG, including session start (see bold text):

```
Apr  5 08:43:14.867: RADIUS:  authenticator 59 7C F3 B8 F4 B2 6A F3 - 29 97 FA E4 CE D5 8B
AF
Apr  5 08:43:14.867: RADIUS:  NAS-IP-Address      [4]   6   10.10.67.2
Apr  5 08:43:14.867: RADIUS:  NAS-Port            [5]   6   0
Apr  5 08:43:14.867: RADIUS:  Vendor, Cisco       [26]  35
Apr  5 08:43:14.867: RADIUS:   cisco-nas-port     [2]   29  "5/0/0/1.300*Virtual-Access1"
Apr  5 08:43:14.867: RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
Apr  5 08:43:14.867: RADIUS:  User-Name           [1]   7   "U0509"
Apr  5 08:43:14.867: RADIUS:  Calling-Station-Id  [31]  7   "U0509"
Apr  5 08:43:14.867: RADIUS:  Acct-Status-Type    [40]  6   Start                     [1]
Apr  5 08:43:14.867: RADIUS:  Acct-Authentic      [45]  6   RADIUS                    [1]
Apr  5 08:43:14.867: RADIUS:  Service-Type        [6]   6   Framed                    [2]
```

```
Apr  5 08:43:14.867: RADIUS:  Acct-Session-Id     [44]  10  "000001A6"
Apr  5 08:43:14.867: RADIUS:  Framed-Protocol     [7]   6   PPP                          [1]
Apr  5 08:43:14.867: RADIUS:  Framed-IP-Address   [8]   6   10.20.81.1
Apr  5 08:43:14.867: RADIUS:  Vendor, Cisco       [26]  24
Apr  5 08:43:14.867: RADIUS:   ssg-account-info   [250] 18  "S10.10.100.11:64"
Apr  5 08:43:14.867: RADIUS:  Vendor, Cisco       [26]  15
Apr  5 08:43:14.867: RADIUS:   ssg-service-info   [251] 9   "NSR0501"
Apr  5 08:43:14.867: RADIUS:  Vendor, Cisco       [26]  14
Apr  5 08:43:14.867: RADIUS:   ssg-service-info   [251] 8   "UU0509"
Apr  5 08:43:14.867: RADIUS:  Vendor, Cisco       [26]  10
Apr  5 08:43:14.867: RADIUS:   ssg-service-info   [251] 4   "TP"
Apr  5 08:43:14.867: RADIUS:  Acct-Delay-Time     [41]  6   0
Apr  5 08:43:14.907: RADIUS: Received from id 1646/173 10.30.81.30:1813,
Accounting-response, len 20
Apr  5 08:43:14.907: RADIUS:  authenticator 53 BD 96 56 B1 39 78 54 - 63 D2 68 C5 0B 99 5F
9A
```

The following example shows a log of accounting activity on the SSG, including watchdog activity (see bold text):

```
Apr  5 08:44:14.895: RADIUS(00000000): Send Accounting-Request to 10.30.81.30:1813 id
1646/175, len 254
Apr  5 08:44:14.895: RADIUS:  authenticator 7A F9 3B F8 16 6F 6C BF - C1 C4 15 AA 9F A2 38
1E
Apr  5 08:44:14.895: RADIUS:  NAS-IP-Address      [4]   6   10.10.67.2
Apr  5 08:44:14.895: RADIUS:  NAS-Port            [5]   6   0
Apr  5 08:44:14.895: RADIUS:  Vendor, Cisco       [26]  35
Apr  5 08:44:14.895: RADIUS:   cisco-nas-port     [2]   29  "5/0/0/1.300*Virtual-Access1"
Apr  5 08:44:14.895: RADIUS:  NAS-Port-Type       [61]  6   Virtual                      [5]
Apr  5 08:44:14.895: RADIUS:  User-Name           [1]   7   "U0509"
Apr  5 08:44:14.895: RADIUS:  Calling-Station-Id  [31]  7   "U0509"
Apr  5 08:44:14.895: RADIUS:  Acct-Status-Type    [40]  6   Watchdog                     [3]
Apr  5 08:44:14.895: RADIUS:  Acct-Authentic      [45]  6   RADIUS                       [1]
Apr  5 08:44:14.895: RADIUS:  Service-Type        [6]   6   Framed                       [2]
Apr  5 08:44:14.895: RADIUS:  Acct-Session-Id     [44]  10  "000001A6"
Apr  5 08:44:14.899: RADIUS:  Acct-Session-Time   [46]  6   60
Apr  5 08:44:14.899: RADIUS:  Acct-Input-Octets   [42]  6   492
Apr  5 08:44:14.899: RADIUS:  Acct-Output-Octets  [43]  6   597
Apr  5 08:44:14.899: RADIUS:  Acct-Input-Packets  [47]  6   5
Apr  5 08:44:14.899: RADIUS:  Acct-Output-Packets [48]  6   6
Apr  5 08:44:14.899: RADIUS:  Framed-Protocol     [7]   6   PPP                          [1]
Apr  5 08:44:14.899: RADIUS:  Framed-IP-Address   [8]   6   10.20.81.1
Apr  5 08:44:14.899: RADIUS:  Vendor, Cisco       [26]  14
Apr  5 08:44:14.899: RADIUS:   ssg-control-info   [253] 8   "I0;492"
Apr  5 08:44:14.899: RADIUS:  Vendor, Cisco       [26]  14
Apr  5 08:44:14.899: RADIUS:   ssg-control-info   [253] 8   "O0;597"
Apr  5 08:44:14.899: RADIUS:  Vendor, Cisco       [26]  24
Apr  5 08:44:14.899: RADIUS:   ssg-account-info   [250] 18  "S10.10.100.11:64"
Apr  5 08:44:14.899: RADIUS:  Vendor, Cisco       [26]  15
Apr  5 08:44:14.899: RADIUS:   ssg-service-info   [251] 9   "NSR0501"
Apr  5 08:44:14.899: RADIUS:  Vendor, Cisco       [26]  14
Apr  5 08:44:14.899: RADIUS:   ssg-service-info   [251] 8   "UU0509"
Apr  5 08:44:14.899: RADIUS:  Vendor, Cisco       [26]  10
Apr  5 08:44:14.899: RADIUS:   ssg-service-info   [251] 4   "TP"
```

The following example shows a log of accounting activity on the SSG, including session stop (see bold text):

```
Apr  5 08:44:42.051: RADIUS/ENCODE: Best Local IP-Address 10.10.67.2 for Radius-Server
10.30.81.30
Apr  5 08:44:42.051: RADIUS(00000000): Send Accounting-Request to 10.30.81.30:1813 id
1646/176, len 260
Apr  5 08:44:42.051: RADIUS:  authenticator AB 80 09 6A E0 C2 FB 3E - B2 75 67 DD 0A FD A3
FA
```

```
Apr  5 08:44:42.051: RADIUS:  NAS-IP-Address      [4]   6   10.10.67.2
Apr  5 08:44:42.051: RADIUS:  NAS-Port            [5]   6   0
Apr  5 08:44:42.051: RADIUS:  Vendor, Cisco       [26]  35
Apr  5 08:44:42.051: RADIUS:   cisco-nas-port     [2]   29  "5/0/0/1.300*Virtual-Access1"
Apr  5 08:44:42.051: RADIUS:  NAS-Port-Type       [61]  6   Virtual                    [5]
Apr  5 08:44:42.051: RADIUS:  User-Name           [1]   7   "U0509"
Apr  5 08:44:42.051: RADIUS:  Calling-Station-Id  [31]  7   "U0509"
Apr  5 08:44:42.051: RADIUS:  Acct-Status-Type    [40]  6   Stop                       [2]
Apr  5 08:44:42.051: RADIUS:  Acct-Authentic      [45]  6   RADIUS                     [1]
Apr  5 08:44:42.051: RADIUS:  Service-Type        [6]   6   Framed                     [2]
Apr  5 08:44:42.051: RADIUS:  Acct-Session-Id     [44]  10  "000001A6"
Apr  5 08:44:42.055: RADIUS:  Acct-Terminate-Cause[49]  6   user-request               [1]
Apr  5 08:44:42.055: RADIUS:  Acct-Session-Time   [46]  6   87
Apr  5 08:44:42.055: RADIUS:  Acct-Input-Octets   [42]  6   492
Apr  5 08:44:42.055: RADIUS:  Acct-Output-Octets  [43]  6   597
Apr  5 08:44:42.055: RADIUS:  Acct-Input-Packets  [47]  6   5
Apr  5 08:44:42.055: RADIUS:  Acct-Output-Packets [48]  6   6
Apr  5 08:44:42.055: RADIUS:  Framed-Protocol     [7]   6   PPP                        [1]
Apr  5 08:44:42.055: RADIUS:  Framed-IP-Address   [8]   6   10.20.81.1
Apr  5 08:44:42.055: RADIUS:  Vendor, Cisco       [26]  14
Apr  5 08:44:42.055: RADIUS:   ssg-control-info   [253] 8   "I0;492"
Apr  5 08:44:42.055: RADIUS:  Vendor, Cisco       [26]  14
Apr  5 08:44:42.055: RADIUS:   ssg-control-info   [253] 8   "O0;597"
Apr  5 08:44:42.055: RADIUS:  Vendor, Cisco       [26]  24
Apr  5 08:44:42.055: RADIUS:   ssg-account-info   [250] 18  "S10.10.100.11:64"
Apr  5 08:44:42.055: RADIUS:  Vendor, Cisco       [26]  15
Apr  5 08:44:42.055: RADIUS:   ssg-service-info   [251] 9   "NSR0501"
Apr  5 08:44:42.055: RADIUS:  Vendor, Cisco       [26]  14
Apr  5 08:44:42.055: RADIUS:   ssg-service-info   [251] 8   "UU0509"
Apr  5 08:44:42.055: RADIUS:  Vendor, Cisco       [26]  10
Apr  5 08:44:42.055: RADIUS:   ssg-service-info   [251] 4   "TP"
Apr  5 08:44:42.055: RADIUS:  Acct-Delay-Time     [41]  6   0
Apr  5 08:44:42.151: RADIUS: Received from id 1646/176 10.30.81.30:1813,
Accounting-response, len 20
Apr  5 08:44:42.151: RADIUS:  authenticator B0 F3 CC 18 67 D5 D2 FD - D5 1C D2 9C EA 3C D4
9D
```

ISG Accounting

There are two methods available to configure accounting update packets for user login and logout, and service start and stop.

1. The first method inserts RADIUS attribute 85 in the subscriber profile, as shown in the following example:

   ```
   Acct-Interim-Interval = 2
   Cisco-AVpair = subscriber:accounting-list=SESM
   ```

   The following ISG configuration command enables AAA accounting of services for billing with a RADIUS server—this is the same command used on the SSG:

   ```
   aaa accounting network SESM start-stop group SESM
   ```

2. The second method for configuring interim accounting works for both PPP and non-PPP sessions. The following RADIUS attribute could be inserted in both a service and subscriber profile:

   ```
   Cisco-AVpair = subscriber:accounting-list=SESM
   ```

   You would configure the following commands on the ISG:

   ```
   aaa accounting update periodic 1
   ```

```
aaa accounting network SESM start-stop group SESM
```

The following examples show logs of accounting activity on the ISG using the **debug aaa accounting** command.

The following example shows activity for session start:

```
Apr  5 09:39:37.148: AAA/ACCT/HC(00007245): PPoA/DE000244 [pre-sess] (rx/tx) adjusted, pre
46/7 call 0/0
Apr  5 09:39:37.148: AAA/ACCT/NET(00007245): Queueing record is START
Apr  5 09:39:37.148: AAA/ACCT(00007245): Accounting method=SESM (RADIUS)
Apr  5 09:39:37.184: AAA/ACCT/NET(00007245): START protocol reply PASS
Apr  5 09:39:37.184: AAA/ACCT(00007245): Send START accounting notification to EM
successfully
Apr  5 09:39:37.184: AAA/ACCT(00007245): Resetting Periodic timer
Apr  5 09:39:37.248: AAA/ACCT/EVENT/(00007245): IPCP_PASS
```

The following example shows watchdog activity:

```
Apr  5 09:40:36.656: AAA/ACCT/CLIENT(00007245): recv 33920000bps xmit 33920000bps
Apr  5 09:40:36.656: AAA/ACCT/HC(00007245): Update PPoA/DE000244
Apr  5 09:40:36.656: AAA/ACCT/HC(00007245): PPoA/DE000244 [sess] (rx/tx) base 0/0 pre 46/7
call 348/183
Apr  5 09:40:36.656: AAA/ACCT/HC(00007245): PPoA/DE000244 [sess] (rx/tx) adjusted, pre
46/7 call 302/176
Apr  5 09:40:36.656: AAA/ACCT/NET(00007245): Queueing record is UPDATE
Apr  5 09:40:36.656: AAA/ACCT(00007245): Sending periodic record type=NET user=U0509
Apr  5 09:40:36.656: AAA/ACCT(00007245): Accounting method=SESM (RADIUS)
Apr  5 09:40:36.728: AAA/ACCT/NET(00007245): UPDATE protocol reply PASS
Apr  5 09:40:36.728: AAA/ACCT(00007245): Send UPDATE accounting notification to EM
successfully
Apr  5 09:40:36.728: AAA/ACCT(00007245): Resetting Periodic timer
```

The following example shows session stop:

```
Apr  5 09:41:14.272: AAA/ACCT/EVENT/(00007249): NET DOWN
Apr  5 09:41:14.272: AAA/ACCT/NET(00007249): Method list not found
Apr  5 09:41:14.272: AAA/ACCT(00007249): del node, session 29377
Apr  5 09:41:14.272: AAA/ACCT/NET(00007249): free_rec, count 0
Apr  5 09:41:14.272: AAA/ACCT/NET(00007249) reccnt 0, csr FALSE, osr 0
Apr  5 09:41:14.272: AAA/ACCT/CLIENT(00007249): recv 33920000bps xmit 33920000bps
Apr  5 09:41:14.272: AAA/ACCT/HC(00007249): Update PPoA/7D000247
Apr  5 09:41:14.272: AAA/ACCT/HC(00007249): PPoA/7D000247 [pre-sess] (rx/tx) base 0/0 pre
0/0 call 0/0
Apr  5 09:41:14.272: AAA/ACCT/HC(00007249): PPoA/7D000247 [pre-sess] (rx/tx) adjusted, pre
0/0 call 0/0
Apr  5 09:41:14.272: AAA/ACCT/CLIENT(00007249): recv 33920000bps xmit 33920000bps
Apr  5 09:41:14.272: AAA/ACCT/HC(00007249): Update PPoA/7D000247
Apr  5 09:41:14.272: AAA/ACCT/HC(00007249): PPoA/7D000247 [sess] (rx/tx) base 0/0 pre 0/0
call 0/0
Apr  5 09:41:14.272: AAA/ACCT/HC(00007249): PPoA/7D000247 [sess] (rx/tx) adjusted, pre 0/0
call 0/0
Apr  5 09:41:14.272: AAA/ACCT/HC(00007249): Deregister PPoA/7D000247
Apr  5 09:41:14.272: AAA/ACCT/EVENT/(00007249): CALL STOP
Apr  5 09:41:14.272: AAA/ACCT(00007249) reccnt 0, osr 0
```

The following examples show a log of accounting activity on the SSG using the **debug aaa accounting** and **radius accounting** commands.

The following log shows activity for session start:

```
Apr  5 12:37:52.561: AAA/ACCT/NET(00007245): Flow id 1 created
Apr  5 12:37:52.561: AAA/ACCT/NET(00007245): add, count 2
Apr  5 12:37:52.561: AAA/ACCT/NET(00007245): Pick method list 'SESM'
Apr  5 12:37:52.561: AAA/ACCT(00007245): Type NET: Periodic timer initialized
```

```
Apr  5 12:37:52.561: AAA/ACCT/EVENT/(00007245): NET UP
Apr  5 12:37:52.561: AAA/ACCT/NET(00007245): Queueing record is START
Apr  5 12:37:52.561: AAA/ACCT(00007245): Accounting method=SESM (RADIUS)
Apr  5 12:37:52.561: RADIUS/ENCODE(00007245):Orig. component type = PPoA
Apr  5 12:37:52.561: RADIUS(00007245): Config NAS IP: 10.10.67.6
Apr  5 12:37:52.561: RADIUS(00007245): sending
Apr  5 12:37:52.561: RADIUS(00007245): Send Accounting-Request to 10.30.81.30:1813 id
1646/4, len 113
Apr  5 12:37:52.561: RADIUS:  authenticator A9 47 BE D1 D7 2F FF 5A - 0E 86 C4 2F FF DF 76
D8
Apr  5 12:37:52.561: RADIUS:  Acct-Session-Id     [44]  10  "000074C3"
Apr  5 12:37:52.561: RADIUS:  Framed-Protocol     [7]   6   PPP                         [1]
Apr  5 12:37:52.561: RADIUS:  Vendor, Cisco       [26]  15
Apr  5 12:37:52.561: RADIUS:   ssg-service-info   [251] 9   "NSR0501"
Apr  5 12:37:52.561: RADIUS:  User-Name           [1]   7   "U0509"
Apr  5 12:37:52.565: RADIUS:  Acct-Status-Type    [40]  6   Start                       [1]
Apr  5 12:37:52.565: RADIUS:  NAS-Port-Type       [61]  6   Virtual                     [5]
Apr  5 12:37:52.565: RADIUS:  NAS-Port            [5]   6   0
Apr  5 12:37:52.565: RADIUS:  NAS-Port-Id         [87]  13  "5/0/0/1.301"
Apr  5 12:37:52.565: RADIUS:  Service-Type        [6]   6   Framed                      [2]
Apr  5 12:37:52.565: RADIUS:  NAS-IP-Address      [4]   6   10.10.67.6
Apr  5 12:37:52.565: RADIUS:  Event-Timestamp     [55]  6   1112704672
Apr  5 12:37:52.565: RADIUS:  Acct-Delay-Time     [41]  6   0
Apr  5 12:37:52.565: RADIUS/ENCODE(00007245):Orig. component type = PPoA
Apr  5 12:37:52.649: RADIUS: Received from id 1646/4 10.30.81.30:1813,
Accounting-response, len 20
Apr  5 12:37:52.649: RADIUS:  authenticator 9E 40 FA ED 45 D3 81 06 - 85 9E 1D EE E4 FF 58
1B
Apr  5 12:37:52.649: AAA/ACCT/NET(00007245): START protocol reply PASS
Apr  5 12:37:52.649: AAA/ACCT(00007245): Send START accounting notification to EM
successfully
Apr  5 12:37:52.649: AAA/ACCT(00007245): Resetting Periodic timer
```

The following example shows watchdog activity (text in bold for purpose of example):

```
Apr  5 12:36:42.857: AAA/ACCT/NET(00007245): Queueing record is UPDATE
Apr  5 12:36:42.857: AAA/ACCT(00007245): Sending periodic record type=NET user=U0509
Apr  5 12:36:42.857: AAA/ACCT(00007245): Accounting method=SESM (RADIUS)
Apr  5 12:36:42.857: RADIUS/ENCODE(00007245):Orig. component type = PPoA
Apr  5 12:36:42.857: RADIUS(00007245): Config NAS IP: 10.10.67.6
Apr  5 12:36:42.857: RADIUS(00007245): sending
Apr  5 12:36:42.857: RADIUS(00007245): Send Accounting-Request to 10.30.81.30:1813 id
1646/1, len 143
Apr  5 12:36:42.857: RADIUS:  authenticator 28 6F 88 46 F9 ED 8C 85 - 1F FB 4F 36 14 D0 D2
BC
Apr  5 12:36:42.857: RADIUS:  Acct-Session-Id     [44]  10  "000072E4"
Apr  5 12:36:42.857: RADIUS:  Framed-Protocol     [7]   6   PPP                         [1]
Apr  5 12:36:42.857: RADIUS:  Vendor, Cisco       [26]  15
Apr  5 12:36:42.857: RADIUS:   ssg-service-info   [251] 9   "NSR0501"
Apr  5 12:36:42.857: RADIUS:  User-Name           [1]   7   "U0509"
Apr  5 12:36:42.857: RADIUS:  Acct-Input-Packets  [47]  6   0
Apr  5 12:36:42.857: RADIUS:  Acct-Output-Packets [48]  6   0
Apr  5 12:36:42.857: RADIUS:  Acct-Input-Octets   [42]  6   0
Apr  5 12:36:42.857: RADIUS:  Acct-Output-Octets  [43]  6   0
Apr  5 12:36:42.857: RADIUS:  Acct-Session-Time   [46]  6   9999
Apr  5 12:36:42.857: RADIUS:  Acct-Status-Type    [40]  6   Watchdog                    [3]
Apr  5 12:36:42.857: RADIUS:  NAS-Port-Type       [61]  6   Virtual                     [5]
Apr  5 12:36:42.857: RADIUS:  NAS-Port            [5]   6   0
Apr  5 12:36:42.857: RADIUS:  NAS-Port-Id         [87]  13  "5/0/0/1.301"
Apr  5 12:36:42.857: RADIUS:  Service-Type        [6]   6   Framed                      [2]
Apr  5 12:36:42.857: RADIUS:  NAS-IP-Address      [4]   6   10.10.67.6
Apr  5 12:36:42.861: RADIUS:  Event-Timestamp     [55]  6   1112704602
Apr  5 12:36:42.861: RADIUS:  Acct-Delay-Time     [41]  6   0
```

```
Apr  5 12:36:42.893: RADIUS: Received from id 1646/1 10.30.81.30:1813,
Accounting-response, len 20
Apr  5 12:36:42.893: RADIUS:  authenticator 6C 7A 02 67 04 0F CB 73 - 21 C8 06 D6 54 FB C8
1F
Apr  5 12:36:42.893: AAA/ACCT/NET(00007245): UPDATE protocol reply PASS
Apr  5 12:36:42.893: AAA/ACCT(00007245): Send UPDATE accounting notification to EM
successfully
Apr  5 12:36:42.893: AAA/ACCT(00007245): Resetting Periodic timer
```

The following example shows service stop:

```
Apr  5 12:37:17.937: AAA/ACCT(00007245): Accounting method=SESM (RADIUS)
Apr  5 12:37:17.937: RADIUS/ENCODE(00007245):Orig. component type = PPoA
Apr  5 12:37:17.937: RADIUS(00007245): Config NAS IP: 10.10.67.6
Apr  5 12:37:17.937: RADIUS(00007245): sending
Apr  5 12:37:17.937: RADIUS(00007245): Send Accounting-Request to 10.30.81.30:1813 id
1646/2, len 181
Apr  5 12:37:17.937: RADIUS:  authenticator 3B 11 0F 7B 92 57 83 15 - B8 6C 2C B2 86 90 D2
31
Apr  5 12:37:17.937: RADIUS:  Acct-Session-Id     [44]  10  "000072E4"
Apr  5 12:37:17.937: RADIUS:  Framed-Protocol     [7]   6   PPP                         [1]
Apr  5 12:37:17.937: RADIUS:  Vendor, Cisco       [26]  15
Apr  5 12:37:17.937: RADIUS:   ssg-service-info   [251] 9   "NSR0501"
Apr  5 12:37:17.937: RADIUS:  User-Name           [1]   7   "U0509"
Apr  5 12:37:17.937: RADIUS:  Acct-Input-Packets  [47]  6   0
Apr  5 12:37:17.937: RADIUS:  Acct-Output-Packets [48]  6   0
Apr  5 12:37:17.937: RADIUS:  Acct-Input-Octets   [42]  6   0
Apr  5 12:37:17.937: RADIUS:  Acct-Output-Octets  [43]  6   0
Apr  5 12:37:17.937: RADIUS:  Acct-Session-Time   [46]  6   10034
Apr  5 12:37:17.937: RADIUS:  Acct-Terminate-Cause[49]  6   none                        [0]
Apr  5 12:37:17.937: RADIUS:  Vendor, Cisco       [26]  32
Apr  5 12:37:17.937: RADIUS:   Cisco AVpair       [1]   26  "disc-cause-ext=No Reason"
Apr  5 12:37:17.937: RADIUS:  Acct-Status-Type    [40]  6   Stop                        [2]
Apr  5 12:37:17.937: RADIUS:  NAS-Port-Type       [61]  6   Virtual                     [5]
Apr  5 12:37:17.937: RADIUS:  NAS-Port            [5]   6   0
Apr  5 12:37:17.937: RADIUS:  NAS-Port-Id         [87]  13  "5/0/0/1.301"
Apr  5 12:37:17.937: RADIUS:  Service-Type        [6]   6   Framed                      [2]
Apr  5 12:37:17.941: RADIUS:  NAS-IP-Address      [4]   6   10.10.67.6
Apr  5 12:37:17.941: RADIUS:  Event-Timestamp     [55]  6   1112704637
Apr  5 12:37:17.941: RADIUS:  Acct-Delay-Time     [41]  6   0
Apr  5 12:37:17.941: RADIUS/ENCODE(00007245):Orig. component type = PPoA
Apr  5 12:37:17.977: RADIUS: Received from id 1646/2 10.30.81.30:1813,
Accounting-response, len 20
Apr  5 12:37:17.977: RADIUS:  authenticator 28 DF AA 20 78 0E AA A7 - 43 72 FD 3B C6 04 5B
E5
Apr  5 12:37:17.977: AAA/ACCT/NET(00007245): STOP protocol reply PASS
Apr  5 12:37:17.977: AAA/ACCT(00007245): Send STOP accounting notification to EM
successfully
Apr  5 12:37:17.977: AAA/ACCT/NET(00007245): Cleaning up from Callback osr 0
Apr  5 12:37:17.977: AAA/ACCT/NET(00007245) Record not present
Apr  5 12:37:17.977: AAA/ACCT/NET(00007245) reccnt 1, csr FALSE, osr 0
```

SSG-to-ISG Migration of Prepaid and Postpaid Services Examples

The following sections compare SSG and ISG prepaid and postpaid services, and provide information that will help you migrate these services:

SSG Basic Prepaid and Postpaid Time- and Volume-Based Services

The SSG Prepaid feature allows SSG to immediately check a subscriber's available credit, to allow or disallow access to certain services. 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.

Prepaid service is defined in a service profile by the Service-Info Z attribute (see bold text in the following example):

```
prepaid-time    Password = "servicecisco", Service-Type = Outbound
   SSG-Service-Info [26,9,251]= "Iprepaid-time",
   SSG-Service-Info [26,9,251]= "R192.168.10.0;255.255.255.0",
   SSG-Service-Info [26,9,251]= "MC",
   SSG-Service-Info [26,9,251]= "TP",
   SSG-Service-Info [26,9,251]= "Z"

prepaid-volume    Password = "servicecisco", Service-Type = Outbound
   SSG-Service-Info [26,9,251]= "Iprepaid-volume",
   SSG-Service-Info [26,9,251]= "R192.168.11.0;255.255.255.0",
   SSG-Service-Info [26,9,251]= "MC",
   SSG-Service-Info [26,9,251]= "TP",
   SSG-Service-Info [26,9,251]= "Z"
```

The prepaid service type is determined by a RADIUS Access-Accept answer from the billing server in reply to the prepaid Authorization-Request sent from the SSG. Time-based prepaid services are defined by the Control-Info QT attribute, and volume-based prepaid services are defined by the Control-Info QV attribute.

When a subscriber logs in to a prepaid service, the SSG sends an authorization Access-Request to the billing server before activating the service, to verify that the subscriber has quota left to use the service. The following example shows a log of the RADIUS Access-Request activity for quota from the SSG to the billing server, for a user named pp-tc71-user1 (key text in bold for purpose of example):

```
RADIUS(00000000): Send Access-Request to 10.30.81.45:1812 id 1645/16, len 142
RADIUS:  authenticator 78 99 C4 5A 5E E7 9E 6D - 01 E0 3D 58 98 F1 76 B6
RADIUS:  User-Name           [1]   15  "pp-tc71-user1"
RADIUS:  User-Password       [2]   18  *
RADIUS:  Calling-Station-Id  [31]  15  "pp-tc71-user1"
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.100.6:64"
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-service-info   [251] 17  "Nprepaid-volume"
RADIUS:  Acct-Session-Id     [44]  10  "00000011"
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.10.100.6
RADIUS:  Event-Timestamp     [55]  6   1112173975
```

The following log is an example of the RADIUS Access-Accept answer from the billing server in response to the billing request from the SSG. The The QV attribute value listed in the following example (in bold text for purpose of example) indicates the user has quota remaining.

```
RADIUS: Received from id 1645/16 10.30.81.45:1812, Access-Accept, len 78
RADIUS:  authenticator C6 41 68 41 1D 95 FD 22 - ED 03 53 ED 91 AF DA 53
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  Class               [25]  14
RADIUS:   70 72 65 70 61 69 64 2D 74 63 37 31              [prepaid-tc71]
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-service-info   [251] 17  "Nprepaid-volume"
RADIUS:  Vendor, Cisco       [26]  15
RADIUS:   ssg-control-info   [253] 9   "QV10000"1
```

If the Control-Info QV or QT attribute is set to 0, the service will not be activated on the SSG. A new authorization request will be sent out from the SSG to the billing server as soon as the subscriber has consumed all of the quota received from the billing server.

Note The following RADIUS-specific configuration commands are applied on the SSG so that some attributes can be inserted in the Access-Request. The following commands insert Cisco AV pairs for attribute 44 (acct-session-id), attribute 55 (UNIX time stamp format), and attribute 25 (class attribute):

```
radius-server attribute 44 include-in-access-req
radius-server attribute 55 access-request include
radius-server attribute 25 access-request include
radius-server vsa send authentication
```

There are several ways to indicate which method list to use for authorization, so the authorization request from the SSG is sent to the correct billing server.

One way is on a virtual template interface using the following configuration commands:

```
interface virtual-template 1
  ppp authorization <method-list name>

aaa authorization network <method-list name> group <radius server-group>

aaa group server radius <radius server-group>
 server <ip address> auth-port [author-port #] acct-port [acct-port #]
```

```
radius-server host <ip add> auth-port [author-port #] acct-port [acct-port #] key <shared
key>
```

A second way is to configure the SSG to use a certain RADIUS server group for prepaid authorization using the following commands:

```
ssg aaa group prepaid <radius server-group>

aaa group server radius <radius server-group>
 server <ip address> auth-port [author-port #] acct-port [acct-port #]

radius-server host <ip add> auth-port [author-port #] acct-port [acct-port #] key <shared
key>
```

When you add the **ssg aaa group prepaid** command to the configuration, the SSG automatically inserts the following command and an internally created and used method list name:

```
aaa authorization network ssg_sg_prepaid_author_internal group <radius server-group>
```

If neither of the two previous methods was used, a default authorization method, such as the following default authorization list configuration, is used:

```
aaa authorization network default group <radius server-group>

aaa group server radius <radius server-group>
 server <ip address> auth-port [author-port #] acct-port [acct-port #]

radius-server host <ip add> auth-port [author-port #] acct-port [acct-port #] key <shared
key>
```

ISG Basic Prepaid and Postpaid Time- and Volume-Based Services

Prepaid service on the ISG is no longer defined by the Service-Info Z attribute, but instead by a Cisco AV pair [26,9,1] with the string "prepaid-config=*prepaid-subscriber-feature-name*." The *prepaid-subscriber-feature-name* supplied in the RADIUS profile is a user-defined name that refers to the same name defined in a local configuration of the prepaid subscriber feature on the ISG. Following are the ISG commands that are entered to configure this feature:

```
subscriber feature prepaid <prepaid subscriber feature name>
 threshold time 0 seconds
 threshold volume 0 bytes
 method-list author <author method-list to use for prepaid author>
 method-list accounting <acct method-list to use for prepaid acct>
 password <password in access-request for prepaid author>
```

There is also a **subscriber feature prepaid default** configuration command available on the ISG that supplies the name "default" for the prepaid subscriber feature. Be aware that this default profile for the subscriber prepaid feature will not appear in the output of the **show running-config** command if none of the default parameters underneath the feature configuration were changed. By default, the prepaid feature configuration is configured as follows:

```
subscriber feature prepaid default
  threshold time 0 seconds
  threshold volume 0 bytes
  method-list authorization default
  method-list accounting default
  password cisco
```

Unless one of the parameters underneath this configuration is changed, you will not see this configuration when looking at the configuration of the router using the **show running-config** command. The following altered default configuration will be visible in the configuration of the router because the method list names were changed:

```
subscriber feature prepaid default
  threshold time 0 seconds
  threshold volume 0 bytes
  method-list authorization rsim-ml
  method-list accounting default rsim-ml
  password servicecisco
```

The method lists created on the ISG for the subscriber prepaid feature profile define which method list to use when a prepaid authorization (such as retrieving quota on the billing server) must be done. The method list indicates to the ISG which RADIUS server group to use, and the server group contains details about the billing server. The ISG works the same way as the SSG in this respect; no changes are required in the AAA part of the configuration.

Following is a partial example of the ISG subscriber prepaid configuration showing new ISG commands (highlighted in bold for purpose of example) to define the method list and the existing AAA commands:

```
.
.
.
subscriber feature prepaid default
 threshold time 0 seconds
 threshold volume 0 bytes
 method-list author rsim-ml-author
 method-list accounting rsim-ml-acct
 password servicecisco

aaa authorization network rsim-ml-author group billing-rsim
aaa accounting network rsim-ml-acct start-stop group billing-rsim

aaa group server radius billing-rsim
 server 10.30.81.45 auth-port 1812 acct-port 1813
 ip radius source-interface Loopback0

radius-server host 10.30.81.45 auth-port 1812 acct-port 1812 key ww
.
.
.
```

For the prepaid functionality to work on the ISG, you *must* insert a *traffic class* into the service profile when defining prepaid service. The traffic class configurations are mandatory and replace the Service-Info R attribute in the SSG prepaid service profile, because the ISG does not interpret this attribute. The following example shows a completely migrated prepaid service profile. Bold text indicates attributes that are added for configuration on the ISG.

```
prepaid-time    Password = "servicecisco", Service-Type = Outbound
   SSG-Service-Info [26,9,251]= "Iprepaid-time",
   SSG-Service-Info [26,9,251]= "R192.168.10.0;255.255.255.0",
   SSG-Service-Info [26,9,251]= "MC",
   SSG-Service-Info [26,9,251]= "TP",
   SSG-Service-Info [26,9,251]= "Z",
   Cisco AV-pair    [26,9,1]  = "prepaid-config=default",
   Cisco AV-pair    [26,9,1]  = "ip:traffic-class=in access-group name prepaid-time-acl
priority 1",
   Cisco AV-pair    [26,9,1]  = "ip:traffic-class=out access-group name prepaid-time-acl
priority 1"

prepaid-volume    Password = "servicecisco", Service-Type = Outbound
```

```
   SSG-Service-Info [26,9,251]= "Iprepaid-volume",
   SSG-Service-Info [26,9,251]= "R192.168.11.0;255.255.255.0",
   SSG-Service-Info [26,9,251]= "MC",
   SSG-Service-Info [26,9,251]= "TP",
   SSG-Service-Info [26,9,251]= "Z",
   Cisco AV-pair    [26,9,1]  = "prepaid-config=default",
   Cisco AV-pair    [26,9,1]  = "ip:traffic-class=in access-group name prepaid-vol-acl
priority 1",
   Cisco AV-pair    [26,9,1]  = "ip:traffic-class=out access-group name prepaid-vol-acl
priority 1"
```

To complete the migration, you must insert extended IP ACLs that are used in the traffic class AV pairs on the ISG. The ACLs replace the Service-Info R attribute value, and are configured as follows:

```
ip access-list extended prepaid-time-acl
 permit ip any 192.168.10.0 255.255.255.0
 permit ip 192.168.10.0 255.255.255.0 any

ip access-list extended prepaid-vol-acl
 permit ip any 192.168.11.0 255.255.255.0
 permit ip 192.168.11.0 255.255.255.0 any
```

The authorization process between the router and the billing server remain the same for both the SSG and ISG. Like the SSG, the ISG sends an authorization request to the billing server before activating the prepaid service for the subscriber, to verify that the subscriber has enough quota remaining to use the service. The Control-Info QV and QT attributes used by the billing server are interpreted the same way by the ISG as they are for the SSG. If the RADIUS Access-Accept answer from the billing server contains a QV value, it is a volume-based prepaid service; if the RADIUS Access-Accept answer from the billing server contains a QT value, it is a time-based prepaid service. If the Control-Info Q attribute value sent by the billing server is zero, the service will be deactivated on the ISG for the corresponding subscriber.

The following log is an example of the RADIUS Access-Request for quota sent from the ISG to the billing server (text highlighted for purpose of example):

```
RADIUS(000000EE): Send Access-Request to 10.30.81.45:1812 id 1645/126, len 149
RADIUS:  authenticator 86 06 D6 96 7F 90 5C 21 - 8D FA D2 F2 8A F2 F1 A6
RADIUS:  User-Name           [1]   15  "pp-tc71-user1"
RADIUS:  User-Password       [2]   18  *
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-service-info   [251] 17  "Nprepaid-volume"
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  NAS-Port            [5]   6   0
RADIUS:  NAS-Port-Id         [87]  13  "3/0/0/0.201"
RADIUS:  Class               [25]  14
RADIUS:   70 72 65 70 61 69 64 2D 74 63 37 31         [prepaid-tc71]
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.10.100.7
RADIUS:  Acct-Session-Id     [44]  10  "00000122"
RADIUS:  Event-Timestamp     [55]  6   1112183844
```

The following example shows a log of the RADIUS Access-Accept answer sent from the billing server to authorize the request sent from the ISG:

```
RADIUS: Received from id 1645/126 10.30.81.45:1812, Access-Accept, len 78
RADIUS:  authenticator 22 7F 0F 01 8A 6E 50 50 - 4B 05 E2 C3 08 0A D8 83
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  Class               [25]  14
RADIUS:   70 72 65 70 61 69 64 2D 74 63 37 31         [prepaid-tc71]
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-service-info   [251] 17  "Nprepaid-volume"
RADIUS:  Vendor, Cisco       [26]  15
```

```
RADIUS:   ssg-control-info   [253] 9   "QV10000"
```

As with the SSG, if the Control-Info QV or QT attribute is set to 0, the service will not be activated on the ISG. A new authorization request will be sent out from the ISG to the billing server as soon as the subscriber has consumed all of the quota received from the billing server.

Note The following RADIUS-specific configuration commands are applied on both the SSG and ISG so that required attributes—attribute 44 (acct-session-id), attribute 55 (UNIX time stamp format), and attribute 25 (class attribute)—are inserted in the Access-Request:

```
radius-server attribute 44 include-in-access-req
radius-server attribute 55 access-request include
radius-server attribute 25 access-request include
radius-server vsa send authentication
```

To verify that a service is activated for a user on the ISG, you must determine whether a unique session ID (uid) was created for the traffic class feature. The uid is associated with the traffic class interface name and the subscriber authenticated name. In the following example, uid 294 identifies the subscriber session, and uid 296 identifies the traffic class created for the prepaid service:

```
Router# show subscriber session

Current Subscriber Information: Total sessions 1

Uniq ID Interface  State          Service      Identifier       Up-time
296     Traffic-Cl unauthen       Ltm Internal pp-tc71-user1    00:13:09
295     Traffic-Cl unauthen       Ltm Internal                  00:18:00
294     Vi4        authen         Local Term   pp-tc71-user1    00:18:00


Router# show subscriber session uid 294

Unique Session ID: 294
Identifier: pp-tc71-user1
SIP subscriber access type(s): PPPoE/PPP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:18:42, Last Changed: 00:13:52
AAA unique ID: 238
Interface: Virtual-Access4

Policy information:
  Context 208C2864: Handle 9400011F
  Authentication status: authen
  Active services associated with session:
    name "prepaid-volume"
    name "prepaid-redirect"
    name "PBHK"
  Rules, actions and conditions executed:
    subscriber rule-map prepaid-user
      condition always event session-start
        1 authenticate aaa list rsim-ml
        2 service-policy type service name PBHK
        3 service-policy type service name prepaid-redirect
    subscriber rule-map prepaid-user
      condition always event service-start
        1 service-policy type service aaa list rsim-ml identifier service-name

Session inbound features:
 Feature: Layer 4 Redirect
  Rule table is empty
```

```
Traffic classes:
  Traffic class session ID: 295
   ACL Name: prepaid-redirect-acl, Packets = 0, Bytes = 0
  Traffic class session ID: 296
   ACL Name: prepaid-vol-acl, Packets = 0, Bytes = 0
 Unmatched Packets (dropped) = 0, Re-classified packets (redirected) = 0

 Feature: Portbundle Hostkey
 Portbundle IP = 10.10.100.7     Bundle Number = 82

Session outbound features:
Traffic classes:
  Traffic class session ID: 295
   ACL Name: prepaid-redirect-acl, Packets = 0, Bytes = 0
  Traffic class session ID: 296
   ACL Name: prepaid-vol-acl, Packets = 0, Bytes = 0
 Unmatched Packets (dropped) = 0, Re-classified packets (redirected) = 0

Configuration sources associated with this session:
Service: prepaid-volume, Active Time = 00:13:53
Service: prepaid-redirect, Active Time = 00:18:43
Service: PBHK, Active Time = 00:18:43
Interface: Virtual-Template2, Active Time = 00:18:43
```

A volume-based service is recognized in the traffic class by the presence of the prepaid volume monitor feature in the **show subscriber session** command details. These features are highlighted in bold in the following example:

```
Router# show subscriber session uid 296

Unique Session ID: 296
Identifier: pp-tc71-user1
SIP subscriber access type(s): Traffic-Class
Current SIP options: None
Session Up-time: 00:14:15, Last Changed: 00:14:15
AAA unique ID: 0

Policy information:
  Context 208C308C: Handle 9B000124
  Authentication status: unauthen
  Prepaid context: default
    threshold time 0 seconds
    threshold volume 0 bytes
    method-list author rsim-ml
    method-list accounting rsim-ml
    password servicecisco
    Interim accounting disabled
    State PREPAID_FEATURE_RUNNING
    Flow idle ? NO
    Total idle time 0 seconds
    Are we accounting for time consumed ? YES
    Acct start sent ? YES

Session inbound features:
 Feature: Prepaid Volume Monitor
   Threshold:10000 - Quota:10000
   Usage(since last update):0 - Total:0
   Current states: Start
Session outbound features:
 Feature: Prepaid Volume Monitor
   Threshold:10000 - Quota:10000
   Usage(since last update):0 - Total:0
   Current states: Start
Configuration sources associated with this session:
```

```
Service: prepaid-volume, Active Time = 00:14:17
```

The counters for usage will be updated periodically when traffic is forwarded to an IP destination matching the ACL configured for the traffic class. As soon as the current usage counter is higher than the threshold, a reauthorization request will be sent to the billing server to retrieve more quota for the service the subscriber is using.

Note The frequency to refresh the usage counters on the traffic class for the prepaid service is not configurable.

A time-based service can be recognized in the traffic class by the presence of the time monitor feature in the **show subscriber session** command details. These features are highlighted in bold in the following example:

```
Router# show subscriber session uid 479

Unique Session ID: 479
Identifier: pp-tc71-user1
SIP subscriber access type(s): Traffic-Class
Current SIP options: None
Session Up-time: 00:00:04, Last Changed: 00:00:04
AAA unique ID: 0

Policy information:
  Context 2078F50C: Handle 80000347
  Authentication status: unauthen
  Prepaid context: default
    threshold time 0 seconds
    threshold volume 0 bytes
    method-list author rsim-ml
    method-list accounting rsim-ml
    password servicecisco
    Interim accounting disabled
    State PREPAID_FEATURE_RUNNING
    Flow idle ? NO
    Total idle time 0 seconds
    Are we accounting for time consumed ? YES
    Acct start sent ? YES

Session inbound features:
 Feature: Prepaid Volume Monitor
   Threshold:4294967295 - Quota:4294967295
   Usage(since last update):0 - Total:0
   Current states: Start
Session outbound features:
 Feature: Prepaid Volume Monitor
   Threshold:4294967295 - Quota:4294967295
   Usage(since last update):0 - Total:0
   Current states: Start
Non-datapath features:
 Feature: Time Monitor
   Threshold: 60 (seconds) - Quota: 60 (seconds)
   Session time: 5 (seconds)
Configuration sources associated with this session:
Service: prepaid-time, Active Time = 00:00:05
```

The next authorization request will be sent as soon as the monitor timer (not visible in the **show** command display) exceeds the threshold time. If you want to see all authorized service for the subscribers and subscriber details, use the **show subscriber session** command with the username, as shown in the following example:

```
Router# show subscriber session username pp-tc71-user1

Unique Session ID: 479
Identifier: pp-tc71-user1
SIP subscriber access type(s): Traffic-Class
Current SIP options: None
Session Up-time: 00:00:04, Last Changed: 00:00:04
AAA unique ID: 0

Policy information:
  Context 2078F50C: Handle 80000347
  Authentication status: unauthen
  Prepaid context: default
    threshold time 0 seconds
    threshold volume 0 bytes
    method-list author rsim-ml
    method-list accounting rsim-ml
    password servicecisco
    Interim accounting disabled
    State PREPAID_FEATURE_RUNNING
    Flow idle ? NO
    Total idle time 0 seconds
    Are we accounting for time consumed ? YES
    Acct start sent ? YES

Session inbound features:
 Feature: Prepaid Volume Monitor
   Threshold:4294967295 - Quota:4294967295
   Usage(since last update):0 - Total:0
   Current states: Start
Session outbound features:
 Feature: Prepaid Volume Monitor
   Threshold:4294967295 - Quota:4294967295
   Usage(since last update):0 - Total:0
   Current states: Start
Non-datapath features:
 Feature: Time Monitor
   Threshold: 60 (seconds) - Quota: 60 (seconds)
   Session time: 5 (seconds)
Configuration sources associated with this session:
Service: prepaid-time, Active Time = 00:00:05

Unique Session ID: 473
Identifier: pp-tc71-user1
SIP subscriber access type(s): PPPoE/PPP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:44:03, Last Changed: 00:00:05
AAA unique ID: 316
Interface: Virtual-Access3

Policy information:
  Context 2078EF9C: Handle E1000336
  Authentication status: authen
  Active services associated with session:
    name "prepaid-time"
    name "prepaid-redirect"
    name "PBHK"
  Rules, actions and conditions executed:
    subscriber rule-map prepaid-user
      condition always event session-start
        1 authenticate aaa list rsim-ml
        2 service-policy type service name PBHK
        3 service-policy type service name prepaid-redirect
    subscriber rule-map prepaid-user
```

```
      condition always event service-start
        1 service-policy type service aaa list rsim-ml identifier service-name

Session inbound features:
 Feature: Layer 4 Redirect
  Rule table is empty
Traffic classes:
  Traffic class session ID: 474
   ACL Name: prepaid-redirect-acl, Packets = 0, Bytes = 0
  Traffic class session ID: 479
   ACL Name: 103, Packets = 19, Bytes = 760
 Unmatched Packets (dropped) = 0, Re-classified packets (redirected) = 0

 Feature: Portbundle Hostkey
 Portbundle IP = 10.10.100.7     Bundle Number = 147

Session outbound features:
Traffic classes:
  Traffic class session ID: 474
   ACL Name: prepaid-redirect-acl, Packets = 0, Bytes = 0
  Traffic class session ID: 479
   ACL Name: 103, Packets = 38, Bytes = 30996
 Unmatched Packets (dropped) = 0, Re-classified packets (redirected) = 0

Configuration sources associated with this session:
Service: prepaid-time, Active Time = 00:00:07
Service: prepaid-redirect, Active Time = 00:44:05
Service: PBHK, Active Time = 00:44:05
Interface: Virtual-Template2, Active Time = 00:44:05
```

The Service-Info PZS attribute defines prepaid server details to use for authorization and can include the IP address, authentication port, accounting port, and the shared key. Following is a sample profile with the Service-Info PZS attributes defined (in bold text for purpose of example):

```
prepaid-remote-ps    Password = "servicecisco", Service-Type = Outbound
   SSG-Service-Info [26,9,251]= "Iprepaid-remote-ps",
   SSG-Service-Info [26,9,251]= "R10.40.96.12;255.255.255.255",
   SSG-Service-Info [26,9,251]= "MC",
   SSG-Service-Info [26,9,251]= "TP",
   SSG-Service-Info [26,9,251]= "Z",
   SSG-Service-Info [26,9,251]= "PZS10.30.81.46;1812;1813;"
```

Note With the SSG, it is possible to insert the details of a different billing server into the prepaid service profile so that the SSG could send the authorization request to this billing server instead of the one configured using the method lists in previous examples.

The Service-Info PZS attributes are not interpreted on the ISG. The functionality must be replaced by defining a new subscriber feature group for the ISG that refers to the method list where the RADIUS server group is configured. This definition will include the same information that is in the PZS Service-Info attribute string, which includes an IP address, authentication port, accounting port, and a shared key.

Bold text in the following example indicates the Cisco AV pair prepaid-config attribute that is added to the profile on the ISG:

```
prepaid-remote-ps    Password = "servicecisco", Service-Type = Outbound
   SSG-Service-Info [26,9,251]= "Iprepaid-remote-ps",
   SSG-Service-Info [26,9,251]= "R10.40.96.12;255.255.255.255",
   SSG-Service-Info [26,9,251]= "MC",
   SSG-Service-Info [26,9,251]= "TP",
```

```
   SSG-Service-Info [26,9,251]= "Z",
   SSG-Service-Info [26,9,251]= "PZS10.30.81.46;1812;1813;"
   Cisco AV-Pair    [26,9,1]  = "ip:traffic-class=in access-group name
prepaid-remote-ps-acl priority 5"
   Cisco AV-Pair    [26,9,1]  = "ip:traffic-class=out access-group name
prepaid-remote-ps-acl priority 5"
   Cisco AV-Pair    [26,9,1]  = "prepaid-config=feat-name-remote-ps-example"
```

The following ISG commands are also added to the configuration to replace the PZS parameters. Notice how these commands use names and addresses defined in the profile.

```
subscriber feature prepaid feat-name-remote-ps-example
 threshold time 0 seconds
 threshold volume 0 bytes
 method-list author prepaid-remote-ps
 method-list accounting prepaid-remote-ps
 password servicecisco

aaa authorization network prepaid-remote-ps group prepaid-remote-ps-sg
aaa accounting network prepaid-remote-ps start-stop group prepaid-remote-ps-sg

aaa group server radius prepaid-remote-ps-sg
 server-private 10.30.81.46 auth-port 1812 acct-port 1813 key cisco
 ip radius source-interface Loopback0
```

SSG Prepaid Threshold

On the SSG, a new authorization request can be sent out to the billing server before the user consumes all of the received quota from the billing server. This type of authorization is done by configuring threshold values using the following commands:

```
Router(config)# ssg prepaid threshold time ?
  <0-6565656>  Threshold time (in seconds)

Router(config)# ssg prepaid threshold volume ?
  <0-65535566>  Threshold volume (in bytes)
```

The values entered in these commands trigger the reauthorization request on the SSG so that if the subscriber receives a time quota value (QT) of 200 seconds and a threshold time of 30 seconds, the reauthorization request is not sent when QT is consumed, but when more than QT minus the threshold value is consumed (200–30=170 seconds). If the threshold value is higher than QT, the reauthorization happens at QT.

ISG Prepaid Threshold

Threshold values are applied on the ISG using **threshold** commands under the subscriber feature prepaid configuration, as shown in the following example (bold text used for purpose of example):

```
subscriber feature prepaid default
 threshold time 0 seconds
 threshold volume 1000 bytes
 method-list author rsim-ml
 method-list accounting rsim-ml
 password servicecisco
```

The ISG **show subscriber session** command with the uid displays the traffic class created for the prepaid service and the calculated threshold value.

```
Router# show subscriber session uid 297

Unique Session ID: 297
Identifier: pp-tc71-user1
SIP subscriber access type(s): Traffic-Class
Current SIP options: None
Session Up-time: 00:00:14, Last Changed: 00:00:14
AAA unique ID: 0

Policy information:
  Context 208C308C: Handle 83000127
  Authentication status: unauthen
  Prepaid context: default
    threshold time 0 seconds
    threshold volume 1000 bytes
    method-list author rsim-ml
    method-list accounting rsim-ml
    password servicecisco
    Interim accounting disabled
    State PREPAID_FEATURE_RUNNING
    Flow idle ? NO
    Total idle time 0 seconds
    Are we accounting for time consumed ? YES
    Acct start sent ? YES

Session inbound features:
 Feature: Prepaid Volume Monitor
 Threshold:9000 - Quota:10000
   Usage(since last update):0 - Total:0
   Current states: Start
Session outbound features:
 Feature: Prepaid Volume Monitor
   Threshold:9000 - Quota:10000
   Usage(since last update):0 - Total:0
   Current states: Start
Configuration sources associated with this session:
Service: prepaid-volume, Active Time = 00:00:15
```

SSG Prepaid Idle Timeout

No additional configuration is needed to apply the Prepaid Idle Timeout feature on an SSG. Prepaid idle timeout is triggered automatically whenever the billing server sends its authorization Access-Accept answer, which contains the quota value given to the subscriber for the prepaid service and the idle timeout attribute (RADIUS attribute 28).

The following log is an example of the Access-Request for quota from the SSG to the billing server (with key information highlighted in bold text):

```
RADIUS(00000000): Send Access-Request to 10.30.81.45:1812 id 1645/27, len 148
RADIUS:  authenticator CE E3 2B 78 3F CB 0E 4A - AB 1E 78 0C 57 49 C3 3A
RADIUS:  User-Name           [1]   15  "pp-tc71-user1"
RADIUS:  User-Password       [2]   18  *
RADIUS:  Calling-Station-Id  [31]  15  "pp-tc71-user1"
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.100.6:64"
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-service-info   [251] 23  "Nprepaid-vol-idletime"
RADIUS:  Acct-Session-Id     [44]  10  "00000032"
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.10.100.6
```

```
RADIUS:  Event-Timestamp     [55]  6   1112199077
```

The following log is an example of the Access-Accept answer from the billing server to the authorization request sent from the SSG (key information is in bold text):

```
RADIUS: Received from id 1645/27 10.30.81.45:1812, Access-Accept, len 90
RADIUS:  authenticator C3 5D 58 AC BE BF 6C 7D - C2 1E 7A 2B AF 57 9A EE
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  Class               [25]  14
RADIUS:   70 72 65 70 61 69 64 2D 74 63 37 31              [prepaid-tc71]
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-service-info   [251] 23  "Nprepaid-vol-idletime"
RADIUS:  Vendor, Cisco       [26]  15
RADIUS:   ssg-control-info   [253] 9   "QV10000"
RADIUS:  Idle-Timeout        [28]  6   300
```

The presence of the idle timer in an authorization Access-Accept answer from the billing server triggers two behaviors on the SSG:

- First is the ability to return allocated quota for the subscriber on the SSG to the billing server whenever the subscriber is idle for a time period equal to the number of seconds set in the Idle-Timeout attribute (attribute 28). In this example, if the subscriber session has not seen traffic for the prepaid service for more than 300 seconds, the SSG will signal via the Control-Info QR1 attribute that the router would like to return the quota because the service has been idle. The QV value in the Access-Request sent from the SSG to the billing server contains the amount of quota already consumed. The SSG will send out a request for quota for this service as soon as the traffic for this prepaid service is resumed.

  The following log is an example of the Access-Request returning quota via QR1 from the SSG to the billing server:

  ```
  RADIUS(00000000): Send Access-Request to 10.30.81.45:1812 id 1645/28, len 170
  RADIUS:  authenticator F8 BA 2A 50 19 C4 EC 0F - 58 B6 0C DA E7 C0 A8 65
  RADIUS:  User-Name           [1]   15  "pp-tc71-user1"
  RADIUS:  User-Password       [2]   18  *
  RADIUS:  Calling-Station-Id  [31]  15  "pp-tc71-user1"
  RADIUS:  Vendor, Cisco       [26]  23
  RADIUS:   ssg-account-info   [250] 17  "S10.10.100.6:64"
  RADIUS:  Vendor, Cisco       [26]  29
  RADIUS:   ssg-service-info   [251] 23  "Nprepaid-vol-idletime"
  RADIUS:  Vendor, Cisco       [26]  11
  RADIUS:   ssg-control-info   [253] 5   "QV325"
  RADIUS:  Vendor, Cisco       [26]  11
  RADIUS:   ssg-control-info   [253] 5   "QR1"
  RADIUS:  Acct-Session-Id     [44]  10  "00000032"
  RADIUS:  Service-Type        [6]   6   Framed                    [2]
  RADIUS:  NAS-IP-Address      [4]   6   10.10.100.6
  RADIUS:  Event-Timestamp     [55]  6   1112199377
  ```

  The following log is an example of the Access-Accept answer from the billing server in response to the Access-Request to return quota from the SSG:

  ```
  RADIUS: Received from id 1645/28 10.30.81.45:1812, Access-Accept, len 86
  RADIUS:  authenticator 18 60 18 5A 20 2A 76 25 - D8 28 F4 B7 82 E4 4D 8B
  RADIUS:  Service-Type        [6]   6   Framed                    [2]
  RADIUS:  Class               [25]  14
  RADIUS:   70 72 65 70 61 69 64 2D 74 63 37 31              [prepaid-tc71]
  RADIUS:  Vendor, Cisco       [26]  29
  RADIUS:   ssg-service-info   [251] 23  "Nprepaid-vol-idletime"
  RADIUS:  Vendor, Cisco       [26]  11
  RADIUS:   ssg-control-info   [253] 5   "QV0"
  RADIUS:  Idle-Timeout        [28]  6   0
  ```

Note In the SSG, the ability to return quota via the QR1 attribute when no traffic is sent for a period longer than the idle timeout value is possible only for volume-based prepaid service, and not for time-based prepaid service.

- The second behavior for idle timeout allows subscribers to replenish their quota within a specific period of time so that service is continued; otherwise, service is disconnected. The SSG sends a reauthorization request to the billing server after a period of time equal to the idle-timeout value present in the authorization request from the billing server.

  The following log is an example of the Access-Request for quota from the SSG to the billing server (with key information highlighted in bold text):

```
Mar 30 17:13:45.421: RADIUS(00000000): Send Access-Request to 10.30.81.45:1812 id
1645/33, len 163
RADIUS:  authenticator EA 52 C5 C5 20 62 E1 D8 - 63 97 51 FA 39 28 9B F8
RADIUS:  User-Name           [1]   15  "pp-tc71-user1"
RADIUS:  User-Password       [2]   18  *
RADIUS:  Calling-Station-Id  [31]  15  "pp-tc71-user1"
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.100.6:64"
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-service-info   [251] 23  "Nprepaid-vol-idletime"
RADIUS:  Vendor, Cisco       [26]  15
RADIUS:   ssg-control-info   [253] 9   "QV20421"
RADIUS:  Acct-Session-Id     [44]  10  "00000043"
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.10.100.6
RADIUS:  Event-Timestamp     [55]  6   1112202825
```

  The following log is an example of the Access-Accept answer from the billing server that indicates to the SSG that the subscriber has no quota remaining (QV is set to 0). Because of the presence of the Idle-Timeout attribute, the SSG is prevented from disconnecting the prepaid service, and will wait to do so until a period of time equal to the idle-timeout value (300 seconds). (Key information is highlighted in bold text for purpose of example.)

```
Mar 30 17:13:45.429: RADIUS: Received from id 1645/33 10.30.81.45:1812, Access-Accept,
len 86
RADIUS:  authenticator 2B 20 34 7B 77 70 4A AA - DC 90 A4 02 35 31 48 F0
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  Class               [25]  14
RADIUS:   70 72 65 70 61 69 64 2D 74 63 37 31         [prepaid-tc71]
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-service-info   [251] 23  "Nprepaid-vol-idletime"
RADIUS:  Vendor, Cisco       [26]  11
RADIUS:   ssg-control-info   [253] 5   "QV0"
RADIUS:  Idle-Timeout        [28]  6   300
```

  Exactly 300 seconds after the billing server informed the SSG that there is no quota left for the subscriber, the SSG will check the billing server again to determine whether the quota was replenished by the subscriber. If QV is still set to 0, the prepaid service will be disconnected. The time stamp in the following example (in bold text) indicates 300 seconds have passed:

```
Mar 30 17:18:45.439: RADIUS(00000000): Send Access-Request to 10.30.81.45:1812 id
1645/34, len 163
RADIUS:  authenticator 6A 86 7E AD BE DA DE E3 - BF 45 32 25 47 D8 AE 17
RADIUS:  User-Name           [1]   15  "pp-tc71-user1"
RADIUS:  User-Password       [2]   18  *
RADIUS:  Calling-Station-Id  [31]  15  "pp-tc71-user1"
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.100.6:64"
```

```
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-service-info   [251] 23  "Nprepaid-vol-idletime"
RADIUS:  Vendor, Cisco       [26]  15
RADIUS:   ssg-control-info   [253] 9   "QV20461"
RADIUS:  Acct-Session-Id     [44]  10  "00000043"
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.10.100.6
RADIUS:  Event-Timestamp     [55]  6   1112203125
```

The following example shows that the subscriber did not replenish quota within the specified idle-timeout period, because the billing server still responds with QV set to 0. The SSG will, therefore, disconnect prepaid service.

```
Mar 30 17:18:45.447: RADIUS: Received from id 1645/34 10.30.81.45:1812, Access-Accept,
len 86
RADIUS:  authenticator 5D C9 C3 AB 44 3E 19 26 - 3A 7C 1A 24 67 04 A5 4A
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  Class               [25]  14
RADIUS:   70 72 65 70 61 69 64 2D 74 63 37 31              [prepaid-tc71]
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-service-info   [251] 23  "Nprepaid-vol-idletime"
RADIUS:  Vendor, Cisco       [26]  11
RADIUS:   ssg-control-info   [253] 5   "QV0"
```

Note The second behavior of SSG—where an Idle-Timeout attribute is sent from the billing server in the authorization accept—applies to both time- and volume-based prepaid services.

ISG Prepaid Idle Timeout

The use of the Idle-Timeout attribute in the authorization accept request from the billing server works the same on the ISG as on the SSG. No additional configuration is needed to enable (trigger) the idle-timeout functionality. The idle timeout is controlled from the billing server itself, whether or not this functionality is triggered on the ISG. This control is enforced when the RADIUS Idle-Timeout attribute (attribute 28) is sent in the RADIUS response message for the remaining quota. The following log is an example of the Access-Request for quota from the ISG to the billing server:

```
RADIUS(00000109): Send Access-Request to 10.30.81.45:1812 id 1645/178, len 155
RADIUS:  authenticator 6C 3A 69 DF 30 F7 9C 4F - FB 7F 02 17 B1 3A 9F 4A
RADIUS:  User-Name           [1]   15  "pp-tc71-user1"
RADIUS:  User-Password       [2]   18  *
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-service-info   [251] 23  "Nprepaid-vol-idletime"
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  NAS-Port            [5]   6   0
RADIUS:  NAS-Port-Id         [87]  13  "3/0/0/0.201"
RADIUS:  Class               [25]  14
RADIUS:   70 72 65 70 61 69 64 2D 74 63 37 31             [prepaid-tc71]
RADIUS:  Service-Type        [6]   6   Framed                   [2]
RADIUS:  NAS-IP-Address      [4]   6   10.10.100.7
RADIUS:  Acct-Session-Id     [44]  10  "00000163"
RADIUS:  Event-Timestamp     [55]  6   1112243253
```

The following log is an example of the Access-Accept answer from the billing server to the authorization request sent from the ISG (see bold text for key information):

```
RADIUS: Received from id 1645/178 10.30.81.45:1812, Access-Accept, len 90
RADIUS:  authenticator 6A 6B 0A E7 2C FE B4 B0 - B2 D0 44 ED 4B 5F 53 69
```

```
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  Class               [25]  14
RADIUS:   70 72 65 70 61 69 64 2D 74 63 37 31              [prepaid-tc71]
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-service-info   [251] 23  "Nprepaid-vol-idletime"
RADIUS:  Vendor, Cisco       [26]  15
RADIUS:   ssg-control-info   [253] 9   "QV10000"
RADIUS:  Idle-Timeout        [28]  6   300
```

To display the traffic class created for the prepaid service and the calculated threshold value, use the ISG **show subscriber session** command with the session uid. Following is sample output with prepaid feature information indicated in bold text:

```
Router# show subscriber session uid 361

Unique Session ID: 361
Identifier: pp-tc71-user1
SIP subscriber access type(s): Traffic-Class
Current SIP options: None
Session Up-time: 00:01:48, Last Changed: 00:01:48
AAA unique ID: 0

Policy information:
  Context 208C2C78: Handle A30001EB
  Authentication status: unauthen
  Prepaid context: default
    threshold time 0 seconds
    threshold volume 1000 bytes
    method-list author rsim-ml
    method-list accounting rsim-ml
    password servicecisco
    Interim accounting disabled
    State PREPAID_FEATURE_RUNNING
    Flow idle ? NO
    Total idle time 0 seconds
    Are we accounting for time consumed ? YES
    Acct start sent ? YES

Session inbound features:
 Feature: Prepaid Idle Timeout
   Timeout configuration: 300 (seconds)
 Feature: Prepaid Volume Monitor
   Threshold:9000 - Quota:10000
   Usage(since last update):4198 - Total:4198
   Current states: Start
Session outbound features:
 Feature: Prepaid Idle Timeout
   Timeout configuration: 300 (seconds)
 Feature: Prepaid Volume Monitor
   Threshold:9000 - Quota:10000
   Usage(since last update):4198 - Total:4198
   Current states: Start
Configuration sources associated with this session:
Service: prepaid-vol-idletime, Active Time = 00:01:49
```

Both behaviors on the SSG for the idle-timeout function (returning and replenishing quota) are also present on the ISG.

The ISG will return the received quota to the billing server if the session was idle for a period longer than the value of the Idle-Timeout attribute (attribute 28), and when the subscriber is not sending IP traffic over the flow of the prepaid service. To signal to the billing server that the ISG wants to return quota, the ISG uses the Control-Info QR1 attribute, the same as for the SSG. Whenever the traffic over the prepaid service flows, the ISG will ask the billing server for quota again.

The following log is an example of the Access-Request returning quota via attribute QR1 from the ISG to the billing server. The prepaid service flow has been idle for more than 300 seconds.

```
RADIUS(00000109): Send Access-Request to 10.30.81.45:1812 id 1645/179, len 180
RADIUS:  authenticator 71 6C C1 2C 32 13 CC 1D - 44 D0 83 B0 5D 9A 5E 9F
RADIUS:  User-Name           [1]   15  "pp-tc71-user1"
RADIUS:  User-Password       [2]   18  *
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-service-info   [251] 23  "Nprepaid-vol-idletime"
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  Vendor, Cisco       [26]  14
RADIUS:   ssg-control-info   [253] 8   "QV4198"
RADIUS:  Vendor, Cisco       [26]  11
RADIUS:   ssg-control-info   [253] 5   "QR1"
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  NAS-Port            [5]   6   0
RADIUS:  NAS-Port-Id         [87]  13  "3/0/0/0.201"
RADIUS:  Class               [25]  14
RADIUS:   70 72 65 70 61 69 64 2D 74 63 37 31              [prepaid-tc71]
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.10.100.7
RADIUS:  Acct-Session-Id     [44]  10  "00000163"
RADIUS:  Event-Timestamp     [55]  6   1112243633
```

The following log is an example of the Access-Accept answer from the billing server in response to the Access-Request to return quota sent by the ISG:

```
RADIUS: Received from id 1645/179 10.30.81.45:1812, Access-Accept, len 86
RADIUS:  authenticator 41 91 09 8B 9E E5 8B A1 - 0B AB 92 B2 F7 83 E3 A1
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  Class               [25]  14
RADIUS:   70 72 65 70 61 69 64 2D 74 63 37 31              [prepaid-tc71]
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-service-info   [251] 23  "Nprepaid-vol-idletime"
RADIUS:  Vendor, Cisco       [26]  11
RADIUS:   ssg-control-info   [253] 5   "QV0"
RADIUS:  Idle-Timeout        [28]  6   0
```

To verify that the flow is idle, use the ISG **show subscriber session** command with the session uid. Following is sample output with key prepaid feature information indicated by bold text:

```
Router# show subscriber session uid 361

Unique Session ID: 361
Identifier: pp-tc71-user1
SIP subscriber access type(s): Traffic-Class
Current SIP options: None
Session Up-time: 00:06:46, Last Changed: 00:00:26
AAA unique ID: 0

Policy information:
  Context 208C2C78: Handle A30001EB
  Authentication status: unauthen
  Prepaid context: default
    threshold time 0 seconds
    threshold volume 1000 bytes
    method-list author rsim-ml
    method-list accounting rsim-ml
    password servicecisco
    Interim accounting disabled
    State PREPAID_FEATURE_RUNNING
    Flow idle ? YES
    Total idle time 300 seconds
    Are we accounting for time consumed ? NO
```

```
    Acct start sent ? YES

Session inbound features:
 Feature: Prepaid Idle Timeout
   Timeout configuration: 300 (seconds)
  Idle Timer is not running
 Feature: Prepaid Volume Monitor
   Threshold:0 - Quota:0
   Usage(since last update):0 - Total:4198
   Current states: Start
Session outbound features:
 Feature: Prepaid Idle Timeout
   Timeout configuration: 300 (seconds)
  Idle Timer is not running
 Feature: Prepaid Volume Monitor
   Threshold:0 - Quota:0
   Usage(since last update):0 - Total:4198
   Current states: Start
Configuration sources associated with this session:
Service: prepaid-vol-idletime, Active Time = 00:06:48
```

Note The ISG does not differ between time- and quota-based services. For both services, the ISG will return quotas if the service is idle for a period longer than the value set for the Idle-Timeout attribute (attribute 28). The SSG does not allow this behavior for time-based services.

The same Idle-Timeout attribute is used for both the SSG and ISG to allow the subscriber to replenish quota within a period of time equal to the idle-timeout value set, assuming all quota has been consumed and the prepaid service has not been disconnected. When the ISG receives an authorization response with an Idle-Timeout attribute from the billing server stating that the subscriber has consumed all available quota, the ISG will start to drop all traffic belonging to the service (or redirect the traffic if configured; see the "ISG Quota Refill Redirection" section on page 75 for more information), but will not clear the subscriber from the connected prepaid service. After a period of time equal to the idle-timeout value, the ISG will send a new authorization request to the billing server, to verify whether the subscriber replenished his quota during this time period.

The following log is an example of the Access-Request for quota sent from the ISG to the billing server. Bold text is used for purpose of example.

```
Mar 31 04:36:24.787: RADIUS(00000109): Send Access-Request to 10.30.81.45:1812 id
1645/182, len 170
RADIUS:  authenticator DC 82 92 A8 2A A6 EB 4E - 0C 55 31 7A 30 28 6E 69
RADIUS:  User-Name           [1]   15  "pp-tc71-user1"
RADIUS:  User-Password       [2]   18  *
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-service-info   [251] 23  "Nprepaid-vol-idletime"
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  Vendor, Cisco       [26]  15
RADIUS:   ssg-control-info   [253] 9   "QV21094"
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  NAS-Port            [5]   6   0
RADIUS:  NAS-Port-Id         [87]  13  "3/0/0/0.201"
RADIUS:  Class               [25]  14
RADIUS:   70 72 65 70 61 69 64 2D 74 63 37 31              [prepaid-tc71]
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.10.100.7
RADIUS:  Acct-Session-Id     [44]  10  "00000163"
RADIUS:  Event-Timestamp     [55]  6   1112243784
```

The following log is an example of the Access-Accept answer from the billing server indicating to the ISG that the subscriber has no quota remaining (QV is set to 0). Because the Idle-Timeout attribute is present, the ISG will not disconnect the prepaid service until a period of time equal to the configured timeout value (300 seconds) has passed. Bold text is used for purpose of example.

```
Mar 31 04:36:24.795: RADIUS: Received from id 1645/182 10.30.81.45:1812, Access-Accept,
len 86
RADIUS:  authenticator F3 93 6A 8B 18 63 D1 46 - 73 07 DE 7F 46 12 79 B5
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  Class               [25]  14
RADIUS:   70 72 65 70 61 69 64 2D 74 63 37 31              [prepaid-tc71]
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-service-info   [251] 23  "Nprepaid-vol-idletime"
RADIUS:  Vendor, Cisco       [26]  11
RADIUS:   ssg-control-info   [253] 5   "QV0"
RADIUS:  Idle-Timeout        [28]  6   300
```

To verify that the state has changed, use the ISG **show subscriber session** command with the session uid. Following is sample output with the prepaid service traffic class information indicated by bold text:

```
Router# show subscriber session uid 361

Unique Session ID: 361
Identifier: pp-tc71-user1
SIP subscriber access type(s): Traffic-Class
Current SIP options: None
Session Up-time: 00:09:20, Last Changed: 00:00:29
AAA unique ID: 0

Policy information:
  Context 208C2C78: Handle A30001EB
  Authentication status: unauthen
  Prepaid context: default
    threshold time 0 seconds
    threshold volume 1000 bytes
    method-list author rsim-ml
    method-list accounting rsim-ml
    password servicecisco
    Interim accounting disabled
    State CREDIT_EXHAUST_TIMER_RUNNING
    Flow idle ? NO
    Total idle time 300 seconds
    Are we accounting for time consumed ? NO
    Acct start sent ? YES

Session inbound features:
 Feature: Prepaid Idle Timeout
   Timeout configuration: 300 (seconds)
 Feature: Prepaid Volume Monitor
   Threshold:4294967295 - Quota:4294967295
   Usage(since last update):0 - Total:21094
   Current states: Start
Session outbound features:
 Feature: Prepaid Idle Timeout
   Timeout configuration: 300 (seconds)
 Feature: Prepaid Volume Monitor
   Threshold:4294967295 - Quota:4294967295
   Usage(since last update):0 - Total:21094
   Current states: Start
Configuration sources associated with this session:
Service: prepaid-vol-idletime, Active Time = 00:09:22
```

Exactly 300 seconds after the billing server informed the ISG that there is no quota left for the subscriber, the ISG will check the billing server again to determine whether the quota was replenished by the subscriber. If QV is still set to 0, the prepaid service will be disconnected. The time stamp in the following example (in bold text for purposes of example) indicates 300 seconds have passed:

```
Mar 31 04:41:24.819: RADIUS(00000109): Send Access-Request to 10.30.81.45:1812 id
1645/183, len 170
RADIUS:  authenticator 1D D7 77 5F FE 41 84 5B - 4F 78 F0 67 FC 8F A1 20
Mar 31 04:41:24.819: RADIUS:  User-Name           [1]   15  "pp-tc71-user1"
Mar 31 04:41:24.819: RADIUS:  User-Password       [2]   18  *
Mar 31 04:41:24.819: RADIUS:  Vendor, Cisco       [26]  29
Mar 31 04:41:24.819: RADIUS:   ssg-service-info   [251] 23  "Nprepaid-vol-idletime"
Mar 31 04:41:24.819: RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
Mar 31 04:41:24.819: RADIUS:  Vendor, Cisco       [26]  15
Mar 31 04:41:24.819: RADIUS:   ssg-control-info   [253] 9   "QV21094"
Mar 31 04:41:24.819: RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
Mar 31 04:41:24.819: RADIUS:  NAS-Port            [5]   6   0
Mar 31 04:41:24.819: RADIUS:  NAS-Port-Id         [87]  13  "3/0/0/0.201"
Mar 31 04:41:24.819: RADIUS:  Class               [25]  14
Mar 31 04:41:24.819: RADIUS:   70 72 65 70 61 69 64 2D 74 63 37 31
[prepaid-tc71]
Mar 31 04:41:24.819: RADIUS:  Service-Type        [6]   6   Framed                    [2]
Mar 31 04:41:24.819: RADIUS:  NAS-IP-Address      [4]   6   10.10.100.7
Mar 31 04:41:24.819: RADIUS:  Acct-Session-Id     [44]  10  "00000163"
Mar 31 04:41:24.819: RADIUS:  Event-Timestamp     [55]  6   1112244084
```

The following example shows that the subscriber did not replenish quota within the specified idle-timeout period, because the billing server still responds with QV set to 0. The ISG will, therefore, disconnect prepaid service.

```
Mar 31 04:41:24.831: RADIUS: Received from id 1645/183 10.30.81.45:1812, Access-Accept,
len 86
Mar 31 04:41:24.831: RADIUS:  authenticator 85 13 E2 91 17 41 5C 21 - 2C BE 41 4E 78 9B 37
82
Mar 31 04:41:24.831: RADIUS:  Service-Type        [6]   6   Framed                    [2]
Mar 31 04:41:24.831: RADIUS:  Class               [25]  14
Mar 31 04:41:24.831: RADIUS:   70 72 65 70 61 69 64 2D 74 63 37 31
[prepaid-tc71]
Mar 31 04:41:24.831: RADIUS:  Vendor, Cisco       [26]  29
Mar 31 04:41:24.831: RADIUS:   ssg-service-info   [251] 23  "Nprepaid-vol-idletime"
Mar 31 04:41:24.831: RADIUS:  Vendor, Cisco       [26]  11
Mar 31 04:41:24.831: RADIUS:   ssg-control-info   [253] 5   "QV0"
```

SSG Dual Quota Prepaid Service

The service authorization response can contain both time and volume quota types. That is, the authorization response can contain both QT and QV attributes. When the SSG receives a service authorization response, it starts both a quota timer and keeps monitoring the connection based on the volume. When either the volume or quota values run out, SSG does a reauthorization. The subsequent authorization request will contain the usage of both quota types in its response. Note that both volume and time quota parameters must be nonzero. The functionality can interwork with the prepaid idle-timeout functionality and volume threshold.

Table 5 shows the different set of actions that the SSG takes when the billing server sends a specific set of values in its authorization response.

Table 5 SSG Dual Quota Prepaid Service Attribute Values and Actions

QT	QV	Idle Timeout	SSG Action
—	—	—	SSG opens the connection. No reauthorization is performed.
0	0	0	SSG opens the connection. Reauthorization occurs when user traffic starts.
0	0	—	SSG closes or does not open the connection.
0	0	>0	SSG opens the connection, but blocks user traffic (drops or redirects it). Reauthorization occurs after a time interval equal to that set for the idle timeout.
-	0	>0	SSG opens the connection, but blocks user traffic (drops or redirects it). Reauthorization occurs after a time interval equal to that set for the idle timeout.
0	>0	0	SSG closes or does not open the connection.
0	>0	>0	SSG closes or does not open the connection.
>0	>0	>0	SSG opens the connection. Reauthorization occurs when QT or QV is consumed, or no user traffic occurs for a time interval equal to that set for the idle timeout.
>0	>0	—	SSG opens the connection. Reauthorization occurs when QT or QV consumed.
>0	>0	0	SSG opens the connection. Reauthorization occurs when QT or QV consumed.
>0	0	>0	SSG opens the connection, but blocks user traffic (drops or redirects it). Reauthorization happens when QT is consumed or after a time interval equal to that set for the idle timeout.
>0	0	0	SSG opens the connection. Reauthorization happens when QT is consumed or when user traffic starts.

ISG Dual Quota Prepaid Service

No special configuration is required on the ISG to convert an SSG prepaid service with dual quota, apart from the conversion of the prepaid service profile on the RADIUS server as described in the "ISG Basic Prepaid and Postpaid Time- and Volume-Based Services" section on page 53. The dual quota behavior is automatically triggered as soon as the billing server sends an authorization to the ISG containing a QT and QV value within a Control-Info attribute. Following is an example of an authorization request for quota sent from the ISG to the billing server. The billing server sends the time and volume quota values in its authorization response; see bold text in the following example:

```
RADIUS(0000013C): Send Access-Request to 10.30.81.45:1812 id 1645/114, len 139
RADIUS:  authenticator 11 15 06 AC F2 9A 8F 6D - AE 27 E9 61 02 C7 10 D3
RADIUS:  User-Name           [1]   15  "pp-tc71-user1"
RADIUS:  User-Password       [2]   18  *
RADIUS:  Vendor, Cisco       [26]  27
RADIUS:   ssg-service-info   [251] 21  "Nprepaid-dual-quota"
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  NAS-Port            [5]   6   0
RADIUS:  NAS-Port-Id         [87]  13  "3/0/0/0.201"
RADIUS:  Service-Type        [6]   6   Framed                    [2]
```

```
RADIUS:  NAS-IP-Address      [4]   6   10.10.100.7
RADIUS:  Acct-Session-Id     [44]  10  "000002BD"
RADIUS:  Event-Timestamp     [55]  6   1113401864
RADIUS: Received from id 1645/114 10.30.81.45:1812, Access-Accept, len 87
RADIUS:  authenticator 1D E7 13 57 7F 55 E3 57 - D5 44 92 B6 5E 94 2E EE
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  Vendor, Cisco       [26]  27
RADIUS:   ssg-service-info   [251] 21  "Nprepaid-dual-quota"
RADIUS:  Vendor, Cisco       [26]  13
RADIUS:   ssg-control-info   [253] 7   "QT180"
RADIUS:  Vendor, Cisco       [26]  15
RADIUS:   ssg-control-info   [253] 9   "QV10000"
RADIUS:  Idle-Timeout        [28]  6   120
```

The presence of both quotas in the authorization response from the billing server will trigger the time and volume monitor features on the traffic class created on the ISG for the prepaid service.

Use the unique session ID created for the traffic class of the prepaid service with the **show subscriber session** command to verify the presence of both the time monitor and volume monitor feature on the traffic class. The following example reveals that both quotas were received from the billing server for this prepaid service (see bold text):

```
Router# show subscriber session uid 486

Unique Session ID: 486
Identifier: pp-tc71-user1
SIP subscriber access type(s): Traffic-Class
Current SIP options: None
Session Up-time: 00:00:17, Last Changed: 00:00:17
AAA unique ID: 0

Policy information:
  Context 2078EB88: Handle D000035B
  Authentication status: unauthen
  Prepaid context: default
    threshold time 0 seconds
    threshold volume 0 bytes
    method-list author rsim-ml
    method-list accounting rsim-ml
    password servicecisco
    Interim accounting disabled
    State PREPAID_FEATURE_RUNNING
    Flow idle ? NO
    Total idle time 0 seconds
    Are we accounting for time consumed ? YES
    Acct start sent ? YES

Session inbound features:
 Feature: Prepaid Idle Timeout
   Timeout configuration: 120 (seconds)
 Feature: Prepaid Volume Monitor
   Threshold:10000 - Quota:10000
   Usage(since last update):0 - Total:0
   Current states: Start
Session outbound features:
 Feature: Prepaid Idle Timeout
   Timeout configuration: 120 (seconds)
 Feature: Prepaid Volume Monitor
   Threshold:10000 - Quota:10000
   Usage(since last update):0 - Total:0
   Current states: Start
Non-datapath features:
 Feature: Time Monitor
```

```
   Threshold: 180 (seconds) - Quota: 180 (seconds)
   Session time: 17 (seconds)
Configuration sources associated with this session:
Service: prepaid-dual-quota, Active Time = 00:00:18
```

The QT value does not work in the same way on the ISG as on the SSG. On the ISG, the value of the QT attribute can be interpreted one of two ways depending upon the presence of the QV attribute, as follows:

- If the QV attribute value is not present in the authorization response and only the QT attribute value is received, the QT value is considered to be a form of quota on the ISG. If the subscriber runs out of this quota, the ISG disconnects the service or blocks and redirects traffic if the idle-timeout value is also present.
- In the dual quota format, the QT attribute value can become a monitor timer: The ISG will check the billing server for quota for the period of time since the last authorization response was received. This period of time is equal to the QT value. If the billing server sends back a QT value equal to 0 and a QV value greater than 0, the monitor timer is turned off on the ISG. The ISG will no longer contact the billing server at the time indicated by the QT value, but rather on other events such as when the idle-timeout value is reached or when the volume is consumed.

The following log shows that the billing server is sending a QT value equal to 0 and a QV value greater than 0 to the ISG in its authorization response (see bold text). In this example, the ISG will not disconnect service (the policy information in the previous **show subscriber session** command output of the traffic class for the prepaid service indicated that the prepaid function was still running). The time monitor will be stopped, and reauthorization at the time specified by the value of the QT attribute will not occur on the ISG. Entering the **show subscriber session** command with the uid of the traffic class for the prepaid service again indicates that the time monitor feature is no longer running (see bold text).

```
RADIUS: Received from id 1645/124 10.30.81.45:1812, Access-Accept, len 85
RADIUS:  authenticator EA DC 81 8D 41 A7 F1 56 - AE 29 AA 51 D8 61 9A 0A
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  Vendor, Cisco       [26]  27
RADIUS:   ssg-service-info   [251] 21  "Nprepaid-dual-quota"
RADIUS:  Vendor, Cisco       [26]  11
RADIUS:   ssg-control-info   [253] 5   "QT0"
RADIUS:  Vendor, Cisco       [26]  15
RADIUS:   ssg-control-info   [253] 9   "QV10000"
RADIUS:  Idle-Timeout        [28]  6   120
RADIUS(0000013F): Received from id 1645/124

Router# show subscriber session uid 489

Unique Session ID: 489
Identifier: pp-tc71-user1
SIP subscriber access type(s): Traffic-Class
Current SIP options: None
Session Up-time: 00:09:45, Last Changed: 00:00:04
AAA unique ID: 0

Policy information:
  Context 2078EB88: Handle 3A000364
  Authentication status: unauthen
  Prepaid context: default
    threshold time 0 seconds
    threshold volume 0 bytes
    method-list author rsim-ml
    method-list accounting rsim-ml
    password servicecisco
    Interim accounting disabled
    State PREPAID_FEATURE_RUNNING
    Flow idle ? NO
    Total idle time 0 seconds
```

```
    Are we accounting for time consumed ? YES
    Acct start sent ? YES

Session inbound features:
 Feature: Prepaid Idle Timeout
   Timeout configuration: 120 (seconds)
 Feature: Prepaid Volume Monitor
   Threshold:10000 - Quota:10000
   Usage(since last update):0 - Total:5610
   Current states: Start
Session outbound features:
 Feature: Prepaid Idle Timeout
   Timeout configuration: 120 (seconds)
 Feature: Prepaid Volume Monitor
   Threshold:10000 - Quota:10000
   Usage(since last update):0 - Total:5610
   Current states: Start
Non-datapath features:
 Feature: Time Monitor
   Threshold: 40 (seconds) - Quota: 40 (seconds)
   Session time: 586 (seconds)
   Monitor Timer is not running
Configuration sources associated with this session:
Service: prepaid-dual-quota, Active Time = 00:09:46
```

Because the QT value behaves differently on the ISG, the actions that the ISG takes upon receiving the authorization answer is slightly different on the ISG compared to the SSG. But as on the SSG, the dual quota functionality on the ISG can still be deployed with other specific prepaid functionality such as prepaid idle timeout and volume threshold.

Table 6 shows the different set of actions that the ISG can take when the billing server sends a specific set of values in its authorization response together with an idle-timeout value.

Table 6 ISG Dual Quota Prepaid Service Attribute Values and Actions

QT	QV	Idle Timeout	ISG Action
0	0	0	ISG opens the traffic class session. Reauthorization occurs when user traffic starts. This all-zero combination should also be noted as the response from the billing server to a quota return authorization request from the ISG using the QR1 attribute. See the "SSG Prepaid Idle Timeout" section on page 62 for more information.
>0	>0	0	ISG opens the traffic class session. Reauthorization occurs when QT or QV is consumed.
>0	0	0	ISG opens the traffic class session. Reauthorization occurs when QT is consumed or when user traffic starts.
—	>0	>0	ISG opens the traffic class session. Reauthorization occurs when QV is consumed, or no user traffic starts for a time interval equal to that set for the idle timeout.
>0	>0	>0	ISG opens the traffic class session. Reauthorization occurs when QT is consumed, or QV is consumed, or no user traffic comes in for a time interval equal to that set for the idle timeout.
—	0	>0	ISG opens the traffic class session, but blocks user traffic (drops or redirects it). Reauthorization occurs after a time interval equal to that set for the idle timeout.

Table 6 ISG Dual Quota Prepaid Service Attribute Values and Actions (continued)

QT	QV	Idle Timeout	ISG Action
0	—	>0	ISG opens the traffic class session, but blocks user traffic (drops or redirects it). Reauthorization occurs after a time interval equal to that set for the idle timeout.
0	0	>0	ISG opens the traffic class session, but blocks user traffic (drops or redirects it). Reauthorization occurs after a time interval equal to that set for the idle timeout.
>0	0	>0	ISG opens the traffic class session, but blocks user traffic (drops or redirects it). Reauthorization occurs when QT is consumed, or after a time interval equal to that set for the idle timeout.

SSG Quota Refill Redirection

Quota refill redirection is applied with prepaid idle timeout functionality on both the SSG and ISG. The idle timer is used to send the reauthorization request to the billing server for a time equal to the value of the idle timeout attribute after the entire quota for the subscriber on the billing server is consumed.

On the SSG, it is possible to redirect all the traffic for a certain prepaid service as soon as the subscriber consumes the entire quota available for the account on the billing server (an event where the QV or QT attribute is set to 0). The service remains up but all subscriber traffic destined for this prepaid service is redirected to a portal server group. This redirection is set up on the SSG using the following commands:

```
ssg tcp-redirect
 server-group prepaid-redirect
  server 10.30.81.22 8097
 redirect prepaid-user to prepaid-redirect
```

On the SSG service profile, there were no additional settings to be inserted; the following example shows the complete profile:

```
pp-quota-refill-vol    Password = "servicecisco", Service-Type = Outbound
   SSG-Service-Info [26,9,251]= "Ipp-quota-refill-vol",
   SSG-Service-Info [26,9,251]= "R10.40.96.5;255.255.255.255",
   SSG-Service-Info [26,9,251]= "MC",
   SSG-Service-Info [26,9,251]= "TP",
   SSG-Service-Info [26,9,251]= "Z",
```

ISG Quota Refill Redirection

To enable quota refill redirection functionality on the ISG, you configure a specific event called credit-exhausted under the policy manager, and apply this event under the L4 Redirect feature.

You must first convert the SSG service profile so it is interpreted on the ISG as a prepaid service. A traffic class is also configured to replace the Service-Info R attribute and complete the prepaid functionality on the ISG.

Note Prioritization *must* be inserted into the traffic class, indicated by an asterisk (*) in the following example profile, to make the redirection work. Prioritization must be configured such that the traffic class used by the L4 redirection service will have a higher priority than the traffic class created for the prepaid service.

The following example converts the previous SSG service pp-quota-refill-vol profile to an ISG profile. Bold text indicates the prepaid and traffic class Cisco AV pair attributes added for the ISG:

```
pp-quota-refill-vol    Password = "servicecisco", Service-Type = Outbound
   SSG-Service-Info [26,9,251]= "Iprepaid-time",
   SSG-Service-Info [26,9,251]= "R10.40.96.5;255.255.255.255",
   SSG-Service-Info [26,9,251]= "MC",
   SSG-Service-Info [26,9,251]= "TP",
   SSG-Service-Info [26,9,251]= "Z",
   Cisco AV-Pair    [26,9,1]  = "prepaid-config=default",
   Cisco AV-Pair    [26,9,1]  = "ip:traffic-class=in access-group name pp-quota-refill-vol
priority 5", (*)
   Cisco AV-Pair    [26,9,1]  = "ip:traffic-class=out access-group name
pp-quota-refill-vol priority 5 "(*)
```

On the ISG, the extended ACL named pp-quota-refill-vol must be inserted into the subscriber prepaid feature configuration. (For the subscriber prepaid feature configuration, see the previous example). The ACL needs to match the value of the Service-Info R attribute. The following example shows the commands used for this configuration:

```
ip access-list extended pp-quota-refill-vol
 permit ip any host 10.40.96.5
 permit ip host 10.40.96.5 any
```

This completes migration of the prepaid service only. The redirection capability now must be introduced into the ISG configuration. The following example shows the commands to configure redirection. Notice how these commands use names and addresses defined in the profile.

```
policy-map type control <control policy-map used by subscriber>
 class type control prepaid-vol-redirect event credit-exhausted
  1 service-policy type service name pp-redict-refill-vol    /*name of service policy map

policy-map type service pp-redict-refill-vol    /*name of service policy map
 class type traffic pp-redirect-refill-vol-tc     /*name of service policy map
  redirect to ip 10.30.81.22 port 8097

class-map type traffic match-any pp-redirect-refill-vol-tc    /*name of service policy map
 match access-group input name pp-redirect-refill-vol    /*name of ACL for traffic class
 match access-group output name pp-redirect-refill-vol

class-map type control match-all prepaid-vol-redirect
 match service-name pp-quota-refill-vol

ip access-list extended pp-redirect-refill-vol    /*name of ACL for traffic class
 permit ip any host 10.40.96.5
 permit ip host 10.40.96.5 any
```

Note The presence of a conditional control statement in the credit-exhaust event under the control policy map used by the subscriber indicates the extended functionality available in the ISG compared to SSG. In the SSG, it is not possible to control what prepaid service is redirected. The ISG allows more control by building a conditional statement into the policy map that defines that actions under which the credit-exhaust event should be executed when this event is triggered from the service named

pp-quota-refill-vol. The credit-exhaust event corresponds to when a prepaid authorization accept request from the billing server is set to zero for one of the available time or volume quotas. The condition is created using a control class map named prepaid-vol-redirect.

Under the credit-exhaust event, an action will trigger a service policy map named pp-redirect-refill-vol. This service is a traffic class that will insert a redirection rule into all the traffic matching the ACL named pp-redirect-refill-vol. The traffic class itself has a priority of 1, which is the highest. No number specified with a **class type traffic** command by default sets priority to 1. In this example, the priority will therefore be preferred over the traffic class for the prepaid service, which has priority set to 5.

Note Do *not* reuse the ACL used for the prepaid service traffic class. Applying different traffic classes with the same ACL name is not allowed in the policy manager. You will see the following message if you try this:

```
Mar 30 15:08:49.883: TC[uid:343]: Another service installed with same ACL, aborting
feature installation
```

If you need to use the same ACL, create a new IP access list name with the same ACL configuration parameters that you used in the ACL for the prepaid service (see the previous example).

To verify your redirection configuration, check the subscriber session uid when the ACL counters are increased, and as soon as the credit-exhaust event has happened and the redirection is applied. Following are examples that display activity before and after the credit-exhaust event, with key information in bold text.

Before the credit-exhaust event, pp-quota-refill-vol class captures all traffic, and the credit-exhaust event occurs because the total quota is consumed. The total quota for the subscriber in this example was set to 20000 bytes. As soon as the usage counter is updated in the prepaid service, the credit-exhaust event will be triggered.

```
Router# show sss session uid 349 | i ACL

   ACL Name: pp-quota-refill-vol, Packets = 102, Bytes = 13761
   ACL Name: pp-quota-refill-vol, Packets = 85, Bytes = 10149
```

After the credit-exhaust event, the L4 redirection traffic class is applied. If the quota refill redirection class is configured correctly, the counters on the ACL for the L4 redirection traffic class should increase. The counters on the traffic class for the prepaid service should remain the same.

```
Router# show sss session uid 349 | i ACL

   ACL Name: pp-quota-refill-vol, Packets = 102, Bytes = 13761
   ACL Name: pp-redirect-refill-vol, Packets = 4, Bytes = 184
   ACL Name: pp-quota-refill-vol, Packets = 85, Bytes = 10149
   ACL Name: pp-redirect-refill-vol, Packets = 8, Bytes = 257
```

The following example shows how to verify what state the prepaid feature is in by checking the session uid for the traffic class created for the prepaid service:

```
Router# show subscriber session uid 353

Unique Session ID: 353
Identifier: pp-tc71-user1
SIP subscriber access type(s): Traffic-Class
Current SIP options: None
Session Up-time: 00:18:03, Last Changed: 00:01:48
AAA unique ID: 0
```

```
Policy information:
  Context 208C2C78: Handle 900001CF
  Authentication status: unauthen
  Prepaid context: default
    threshold time 0 seconds
    threshold volume 1000 bytes
    method-list author rsim-ml
    method-list accounting rsim-ml
    password servicecisco
    Interim accounting disabled
    State CREDIT_EXHAUST_TIMER_RUNNING
    Flow idle ? NO
    Total idle time 0 seconds
    Are we accounting for time consumed ? NO
    Acct start sent ? YES

Session inbound features:
 Feature: Prepaid Idle Timeout
   Timeout configuration: 300 (seconds)
 Feature: Prepaid Volume Monitor
   Threshold:4294967295 - Quota:4294967295
   Usage(since last update):0 - Total:23910
   Current states: Start
Session outbound features:
 Feature: Prepaid Idle Timeout
   Timeout configuration: 300 (seconds)
 Feature: Prepaid Volume Monitor
   Threshold:4294967295 - Quota:4294967295
   Usage(since last update):0 - Total:23910
   Current states: Start
Configuration sources associated with this session:
Service: pp-quota-refill-vol, Active Time = 00:18:20
```

Note The combination of L4 redirection and traffic classification is currently affected by limitations described in the "CSCeh35036—Two Traffic Classes with L4 Redirect Do Not Work" section on page 91: Two traffic classes on which prioritization and L4 redirection are applied, and for which the ACLs used to do the traffic classification overlap, cannot be used at the same time. Return traffic will fail to get translated when it is translated using the traffic class service that was last applied.

Note The L4 redirection service applied at the credit-exhaust event is unapplied on the ISG, regardless of the authorization request received by the billing server upon expiration idle-timeout value. This redirection is triggered by an internal event in the policy manager (shown in debugging messages as "internal-event-cre-t-exp"), and this internal event will unapply all the actions applied to the subscriber during the credit-exhaust event.

SSG Tariff Switching: Postpaid Services

A postpaid service is different from a prepaid service in that there is no authorization request for quota sent to the billing server. The service profile for a postpaid service contains a weekly tariff switch plan containing the various tariff switch points within the week, configured using the Service-Info PPW attribute. The SSG monitors the usage at every tariff switch point and records this information in the interim accounting records, configured using the Control-Info QB attribute. The billing server monitors

all accounting interim updates and obtains the information about the volume of traffic sent during the various tariff switching periods. Following is a sample service profile with the Service-Info PPW attribute highlighted for purpose of example:

```
postpaid-tariff-sw    Password = "servicecisco", Service-Type = Outbound
   SSG-Service-Info [26,9,251]= "Ipostpaid-tariff-sw",
   SSG-Service-Info [26,9,251]= "R10.40.96.10;255.255.255.255",
   SSG-Service-Info [26,9,251]= "MC",
   SSG-Service-Info [26,9,251]= "TP",
   SSG-Service-Info [26,9,251]= "PPW12:00:00:31"
```

To enable interim accounting on the SSG for services, configure the **ssg accounting per-service interval** command. The interval value is set in minutes.

```
ssg accounting per-service interval 2
```

Note It is also possible to activate interim accounting for the service by including the Service-Info L attribute in the service profile (for example, SSG-Service-Info [26, 9, 251] = "L120,enable").

ISG Tariff Switching: Postpaid Services

To indicate the weekly tariff switch plan for a postpaid service on the ISG, use the same Service-Info PPW attribute as used on the SSG. The ISG interim accounting and stop records will also contain the same Control-Info QB attribute to signal the time when the last tariff switch occurred, together with the total amount of bytes sent since the last tariff switch time.

To force the ISG to send out RADIUS start and stop accounting packets for the postpaid service, you must insert the accounting-list subscriber Cisco AV pair in the service profile (shown in bold text for purpose of example):

```
postpaid-tariff-sw    Password = "servicecisco", Service-Type = Outbound
   SSG-Service-Info [26,9,251]= "Ipostpaid-tariff-sw",
   SSG-Service-Info [26,9,251]= "R10.40.96.10;255.255.255.255",
   SSG-Service-Info [26,9,251]= "MC",
   SSG-Service-Info [26,9,251]= "TP",
   SSG-Service-Info [26,9,251]= "PPW12:00:00:31",
   Cisco AV-Pair    [26,9,1]  = "subscriber:accounting-list=<acct method-list>"
```

To make certain that the Control-Info QB attribute values are present in the interim accounting start and stop packets, you must enable interim accounting. The SSG attributes that triggered interim accounting are not interpreted on the ISG. There are two methods available to enable interim accounting on the ISG.

1. Insert RADIUS attribute 85 value (acct-interim-interval; value in seconds) on the subscriber profile. Do not insert this attribute on the service profile because this action will not enable the interim accounting behavior on the service. This problem is addressed in the "CSCeh03451—Periodic Accounting on Flows Behaves Inconsistently in the ISG" section on page 90.

Note RADIUS attribute 85 works only on PPP sessions, not IP sessions.

2. Enable periodic accounting using the **aaa accounting update periodic** command. The update period value is set in minutes.

   ```
   aaa accounting update periodic 2
   ```

This command enables periodic accounting on each session and flow that has the VSA accounting pair in its profile.

The following log is an example of interim accounting packet activity before tariff switching is enabled—that is, the tariff switch time is set to 0, the service has started, but no tariff switching has occurred on the service.

```
RADIUS(000000CD): Send Accounting-Request to 10.30.81.45:1813 id 1646/57, len 194
RADIUS:  authenticator 7F 25 BA DE 57 67 17 FF - 2E DC A7 D8 B2 DC 90 A8
RADIUS:  Acct-Session-Id     [44]  10  "000000D1"
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  Vendor, Cisco       [26]  27
RADIUS:   ssg-service-info   [251] 21  "Npostpaid-tariff-sw"
RADIUS:  Vendor, Cisco       [26]  17
RADIUS:   ssg-control-info   [253] 11  "QB11246;0"
RADIUS:  User-Name           [1]   15  "pp-tc71-user1"
RADIUS:  Acct-Input-Packets  [47]  6   48
RADIUS:  Acct-Output-Packets [48]  6   40
RADIUS:  Acct-Input-Octets   [42]  6   6470
RADIUS:  Acct-Output-Octets  [43]  6   4776
RADIUS:  Acct-Session-Time   [46]  6   2971
RADIUS:  Acct-Status-Type    [40]  6   Watchdog                  [3]
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  NAS-Port            [5]   6   0
RADIUS:  NAS-Port-Id         [87]  13  "3/0/0/0.201"
RADIUS:  Class               [25]  14
RADIUS:   70 72 65 70 61 69 64 2D 74 63 37 31              [prepaid-tc71]
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.10.100.7
RADIUS:  Event-Timestamp     [55]  6   1112706015
RADIUS:  Acct-Delay-Time     [41]  6   0
```

Once tariff switching occurs, the QB attribute will indicate the amount of bytes sent after the last tariff switch and the time when tariff switching occurred in UNIX time stamp format.

Use the **show subscriber session** command to display the uid created for the traffic class used for the tariff switching service, as follows (shown in bold text for purpose of example):

```
Router# show subscriber session uid 209

Unique Session ID: 209
Identifier:
SIP subscriber access type(s): Traffic-Class
Current SIP options: None
Session Up-time: 00:56:14, Last Changed: 00:56:14
AAA unique ID: 0

Policy information:
  Context 2078EB88: Handle 6700001B
  Authentication status: unauthen

Session inbound features:
 Feature: Service accounting
  Service: postpaid-tariff-sw
  Method List: rsim-ml
  Weekly tariff plan: 14:00:00:31
  Packets = 48, Bytes = 6470

Session outbound features:
 Feature: Service accounting
  Service: postpaid-tariff-sw
  Method List: rsim-ml
  Weekly tariff plan: 14:00:00:31
  Packets = 40, Bytes = 4776
```

```
Configuration sources associated with this session:
Service: postpaid-tariff-sw, Active Time = 00:56:14
```

The following log is an example of the accounting interim update after tariff switch time occurs (key fields are highlighted in bold text for purpose of example):

```
RADIUS(000000CD): Send Accounting-Request to 10.30.81.45:1813 id 1646/68, len 202
RADIUS:  authenticator 47 65 47 03 96 DB 4B 3B - A8 83 0A E6 55 5C 08 A8
RADIUS:  Acct-Session-Id     [44]  10  "000000D1"
RADIUS:  Framed-Protocol     [7]   6   PPP                        [1]
RADIUS:  Vendor, Cisco       [26]  27
RADIUS:   ssg-service-info   [251] 21  "Npostpaid-tariff-sw"
RADIUS:  Vendor, Cisco       [26]  25
RADIUS:   ssg-control-info   [253] 19  "QB2818;1112706000"
RADIUS:  User-Name           [1]   15  "pp-tc71-user1"
RADIUS:  Acct-Input-Packets  [47]  6   60
RADIUS:  Acct-Output-Packets [48]  6   50
RADIUS:  Acct-Input-Octets   [42]  6   8094
RADIUS:  Acct-Output-Octets  [43]  6   5970
RADIUS:  Acct-Session-Time   [46]  6   3536
RADIUS:  Acct-Status-Type    [40]  6   Watchdog                   [3]
RADIUS:  NAS-Port-Type       [61]  6   Virtual                    [5]
RADIUS:  NAS-Port            [5]   6   0
RADIUS:  NAS-Port-Id         [87]  13  "3/0/0/0.201"
RADIUS:  Class               [25]  14
RADIUS:   70 72 65 70 61 69 64 2D 74 63 37 31              [prepaid-tc71]
RADIUS:  Service-Type        [6]   6   Framed                     [2]
RADIUS:  NAS-IP-Address      [4]   6   10.10.100.7
RADIUS:  Event-Timestamp     [55]  6   1112706580
RADIUS:  Acct-Delay-Time     [41]  6   0
```

The following log is an example of the accounting stop record. The QB attribute is present and its value equals the amount of bytes sent since the last tariff switch (key fields are highlighted in bold text for purpose of example):

```
RADIUS: Send Accounting-Request to 10.30.81.45:1813 id 1646/104, len 243
RADIUS:  authenticator 31 D9 2F 21 47 D1 87 AE - 44 2E 1E A5 77 C5 41 8C
RADIUS:  Acct-Session-Id     [44]  10  "000000D1"
RADIUS:  Framed-Protocol     [7]   6   PPP                        [1]
RADIUS:  Vendor, Cisco       [26]  27
RADIUS:   ssg-service-info   [251] 21  "Npostpaid-tariff-sw"
RADIUS:  Vendor, Cisco       [26]  25
RADIUS:   ssg-control-info   [253] 19  "QB2818;1112706000"
RADIUS:  User-Name           [1]   15  "pp-tc71-user1"
RADIUS:  Acct-Input-Packets  [47]  6   60
RADIUS:  Acct-Output-Packets [48]  6   50
RADIUS:  Acct-Input-Octets   [42]  6   8094
RADIUS:  Acct-Output-Octets  [43]  6   5970
RADIUS:  Acct-Session-Time   [46]  6   5594
RADIUS:  Acct-Terminate-Cause[49]  6   user-request               [1]
RADIUS:  Vendor, Cisco       [26]  35
RADIUS:   Cisco AVpair       [1]   29  "disc-cause-ext=TS User Exit"
RADIUS:  Acct-Status-Type    [40]  6   Stop                       [2]
RADIUS:  NAS-Port-Type       [61]  6   Virtual                    [5]
RADIUS:  NAS-Port            [5]   6   0
RADIUS:  NAS-Port-Id         [87]  13  "3/0/0/0.201"
RADIUS:  Class               [25]  14
RADIUS:   70 72 65 70 61 69 64 2D 74 63 37 31              [prepaid-tc71]
RADIUS:  Service-Type        [6]   6   Framed                     [2]
RADIUS:  NAS-IP-Address      [4]   6   10.10.100.7
RADIUS:  Event-Timestamp     [55]  6   1112708638
RADIUS:  Acct-Delay-Time     [41]  6   01
```

SSG Tariff Switching: Prepaid Services

The prepaid tariff switching feature enhances the SSG prepaid capability by bringing in the flexibility of supporting changes in tariffs during the lifetime of a connection. This feature applies to the volume-based prepaid connections wherein the rate of charging would vary depending upon the time of service access. With this feature, SSG will be able to monitor the prepaid connection based on volume and, at tariff switching time, will be able to switch to the new tariff scheme. On the SSG, no additional configuration is done to insert the tariff switching functionality on the prepaid service in question. This functionality is signaled by the prepaid billing server in its authorization response to the SSG. The response includes the tariff change time and the tokens for postswitch and preswitch periods. The values for these different parameters are inserted into a string with the following format in the Control-Info attribute [26,9,253]:

```
"QX<seconds before switch>;<preswitch volume in bytes>;<postswitch volume in bytes>"
```

To indicate to the billing server how much volume quota was consumed in the period before and after the tariff switch, the SSG uses the following string format in Control-Info attribute [26,9,253]:

```
"QB<total amount of volume consumed after last tariff switch>;<tariff switch time in UNIX
time-stamp>"
```

The previous VSA can be present in reauthorization requests, accounting interim updates, and accounting stop packets. Note that this will be in addition to the usual quota volume attribute that indicates the total volume usage in that connection.

As for the postpaid functionality, this service type requires the usage of interim accounting on the SSG to make it possible on the ISG to retrieve the information of usage in the various intervals because of the tariff switch. To have an accounting interim update in every tariff switch interval, the accounting interim update interval must be less than the tariff switch interval.

The prepaid tariff switching functionality can interwork with the prepaid idle-timeout functionality and volume threshold.

Table 7 shows the different set of actions that the SSG takes when the billing server sends a specific set of values in its authorization response.

Table 7 SSG Tariff Switching Attribute Values and Actions

QT	QX, tariff switching, preswitch (PRE), postswitch (POST)	Idle Timeout	SSG Action
0	>0;0;0	0	SSG opens the connection. Reauthorization occurs when user traffic starts.
0	>0;0;0	>0	SSG opens the connection, but blocks user traffic (drops or redirects it). Reauthorization occurs after a time interval equal to that set for the idle timeout.
0	Any combination not covered by previous two value sets	0 or >0	SSG closes or does not open the connection.

Table 7 SSG Tariff Switching Attribute Values (continued) and Actions (continued)

QT	QX, tariff switching, preswitch (PRE), postswitch (POST)	Idle Timeout	SSG Action
>0	>0;>0;>0	>0	SSG opens the connection. Reauthorization occurs when QT is consumed, or PRE is consumed before tariff switching, or when PRE plus POST are consumed, or no user traffic for a time interval equal to that set for the idle timeout.
>0	>0;>0;0	>0	SSG opens the connection. Reauthorization occurs when QT is consumed, or PRE is consumed before tariff switching, or when tariff switching occurs, or no user traffic for a time interval equal to that set for the idle timeout.
>0	>0;>0;>0	0	SSG opens the connection. Reauthorization occurs when QT is consumed, or PRE is consumed before tariff switching, or when PRE plus POST are consumed.
>0	>0;>0;0	0	SSG opens the connection. Reauthorization occurs when QT is consumed, or PRE is consumed before tariff switching, or when tariff switching occurs.
>0	>0;0;0	0	SSG opens the connection. Reauthorization occurs when QT is consumed or when user traffic starts.

ISG Tariff Switching: Prepaid Services

As with the SSG, it is possible to trigger the prepaid tariff switch method on a prepaid service on the ISG. The ISG interprets or uses the same VSA attributes and string formats for this purpose as those used on the SSG. No additional commands or migration steps are required to migrate from the SSG to the ISG, apart from adjusting the prepaid service profile as described in the "ISG Basic Prepaid and Postpaid Time- and Volume-Based Services" section on page 53). As soon as the billing server indicates a tariff switch interval coming up by inserting the QX attribute in an authorization response, the prepaid tariff switching functionality will be triggered on the ISG.

The following log shows how the billing server indicates to the ISG that there is a tariff switch period coming up for the prepaid service by using the QX attribute. The **show subscriber session uid 498** command reports that the traffic class of this prepaid service contains information about an upcoming tariff switch period (key fields are highlighted in bold text for purpose of example).

```
RADIUS(00000143): Send Access-Request to 10.30.81.45:1812 id 1645/138, len 165
RADIUS:  authenticator EC 3D 59 91 82 29 32 E5 - AE 27 E9 61 8F 5C F2 66
RADIUS:  User-Name           [1]   15  "pp-tc71-user1"
RADIUS:  User-Password       [2]   18  *
RADIUS:  Vendor, Cisco       [26]  26
RADIUS:   ssg-service-info   [251] 20  "Npp-tariff-sw-time"
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  Vendor, Cisco       [26]  12
RADIUS:   ssg-control-info   [253] 6   "QT45"
RADIUS:  Vendor, Cisco       [26]  15
RADIUS:   ssg-control-info   [253] 9   "QV10605"
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  NAS-Port            [5]   6   0
```

```
RADIUS:  NAS-Port-Id         [87]  13  "3/0/0/0.201"
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.10.100.7
RADIUS:  Acct-Session-Id     [44]  10  "000002D2"
RADIUS:  Event-Timestamp     [55]  6   1113489476
RADIUS: Received from id 1645/138 10.30.81.45:1812, Access-Accept, len 91
RADIUS:  authenticator 53 1F 61 87 C9 AD 8E 0E - EF C4 8A 65 98 D4 43 E5
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  Vendor, Cisco       [26]  26
RADIUS:   ssg-service-info   [251] 20  "Npp-tariff-sw-time"
RADIUS:  Vendor, Cisco       [26]  14
RADIUS:   ssg-control-info   [253] 8   "QT3600"
RADIUS:  Vendor, Cisco       [26]  25
RADIUS:   ssg-control-info   [253] 19  "QX399;10000;18790"
RADIUS(00000143): Received from id 1645/138

Router# show subscriber session uid 498

Unique Session ID: 498
Identifier: pp-tc71-user1
SIP subscriber access type(s): Traffic-Class
Current SIP options: None
Session Up-time: 00:01:01, Last Changed: 00:00:16
AAA unique ID: 0

Policy information:
  Context 2078EB88: Handle 4C000381
  Authentication status: unauthen
  Prepaid context: default
    threshold time 0 seconds
    threshold volume 0 bytes
    method-list author rsim-ml
    method-list accounting rsim-ml
    password servicecisco
    Interim accounting disabled
    State PREPAID_FEATURE_RUNNING
    Flow idle ? NO
    Total idle time 0 seconds
    Are we accounting for time consumed ? YES
    Acct start sent ? YES

Session inbound features:
 Feature: Service accounting
  Service: pp-tariff-sw-time
  Method List: rsim-ml
  Packets = 54, Bytes = 7273

Feature: Prepaid Volume Monitor
   Threshold:10000 - Quota:10000
   Post Tariff Threshold:18790 - Quota:18790
   Usage(since last update):2041 - Total:12646
   Current states: Start
Session outbound features:
 Feature: Service accounting
  Service: pp-tariff-sw-time
  Method List: rsim-ml
  Packets = 45, Bytes = 5373

 Feature: Prepaid Volume Monitor
   Threshold:10000 - Quota:10000
   Post Tariff Threshold:18790 - Quota:18790
   Usage(since last update):2041 - Total:12646
   Current states: Start
Non-datapath features:
```

```
 Feature: Time Monitor
   Threshold: 3600 (seconds) - Quota: 3600 (seconds)
   Session time: 62 (seconds)
Configuration sources associated with this session:
Service: pp-tariff-sw-time, Active Time = 00:01:03
```

The previous example indicates that the tariff switch must take place after 399 seconds.

The following **show subscriber session** command output indicates that tariff switching happened, because the traffic class for the prepaid service is now starting to use the posttariff switch quota on the ISG (key fields are highlighted in bold text for purpose of example):

```
Router# show subscriber session uid 498

Unique Session ID: 498
Identifier: pp-tc71-user1
SIP subscriber access type(s): Traffic-Class
Current SIP options: None
Session Up-time: 00:08:07, Last Changed: 00:07:22
AAA unique ID: 0

Policy information:
  Context 2078EB88: Handle 4C000381
  Authentication status: unauthen
  Prepaid context: default
    threshold time 0 seconds
    threshold volume 0 bytes
    method-list author rsim-ml
    method-list accounting rsim-ml
    password servicecisco
    Interim accounting disabled
    State PREPAID_FEATURE_RUNNING
    Flow idle ? NO
    Total idle time 0 seconds
    Are we accounting for time consumed ? YES
    Acct start sent ? YES

Session inbound features:
 Feature: Service accounting
  Service: pp-tariff-sw-time
  Method List: rsim-ml
  Packets = 60, Bytes = 8084

 Feature: Prepaid Volume Monitor
   Threshold:10000 - Quota:10000
   Post Tariff Threshold:18790 - Quota:18790
   Usage(since last update):0 - Total:14054
   Current states: Start Tariff-switched
Session outbound features:
 Feature: Service accounting
  Service: pp-tariff-sw-time
  Method List: rsim-ml
  Packets = 50, Bytes = 5970

 Feature: Prepaid Volume Monitor
   Threshold:10000 - Quota:10000
   Post Tariff Threshold:18790 - Quota:18790
   Usage(since last update):0 - Total:14054
   Current states: Start Tariff-switched
Non-datapath features:
 Feature: Time Monitor
   Threshold: 3600 (seconds) - Quota: 3600 (seconds)
   Session time: 488 (seconds)
Configuration sources associated with this session:
```

```
Service: pp-tariff-sw-time, Active Time = 00:08:09
```

To send out a new authorization to the billing server, the threshold for the volume quota usage must exceed the Post Tariff Threshold value when the tariff switch happened.

Just as on the SSG, the accounting interim updates must contain the QB parameter to indicate to the billing server how much quota of the total consumed quota (QV) was consumed after the tariff switch time. See the bold text in the following example:

```
RADIUS(00000143): Send Accounting-Request to 10.30.81.45:1813 id 1646/68, len 212
RADIUS:  authenticator CE 19 23 2C 0B 35 2E 63 - 45 59 1E 96 75 78 39 6E
RADIUS:  Acct-Session-Id     [44]  10  "000002D2"
RADIUS:  Vendor, Cisco       [26]  26
RADIUS:   ssg-service-info   [251] 20  "Npp-tariff-sw-time"
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  Framed-IP-Address   [8]   6   10.20.72.10
RADIUS:  User-Name           [1]   15  "pp-tc71-user1"
RADIUS:  Vendor, Cisco       [26]  25
RADIUS:   ssg-control-info   [253] 19  "QB8448;1113489875"
RADIUS:  Vendor, Cisco       [26]  16
RADIUS:   ssg-control-info   [253] 10  "I0;12950"
RADIUS:  Vendor, Cisco       [26]  15
RADIUS:   ssg-control-info   [253] 9   "O0;9552"
RADIUS:  Acct-Input-Octets   [42]  6   12950
RADIUS:  Acct-Output-Octets  [43]  6   9552
RADIUS:  Acct-Session-Time   [46]  6   552
RADIUS:  Acct-Status-Type    [40]  6   Watchdog                  [3]
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  NAS-Port            [5]   6   0
RADIUS:  NAS-Port-Id         [87]  13  "3/0/0/0.201"
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.10.100.7
RADIUS:  Event-Timestamp     [55]  6   1113489983
RADIUS:  Acct-Delay-Time     [41]  6   0
```

To understand how to trigger interim accounting updates, see the "ISG Basic Prepaid and Postpaid Time- and Volume-Based Services" section on page 53.

The QB value can also be inserted in the authorization request sent by the ISG to the billing server, as highlighted text in the following example indicates:

```
RADIUS(00000143): Send Access-Request to 10.30.81.45:1812 id 1645/139, len 192
RADIUS:  authenticator EC 3D 59 91 82 29 32 E5 - AE 27 E9 61 8F 5C F2 66
RADIUS:  User-Name           [1]   15  "pp-tc71-user1"
RADIUS:  User-Password       [2]   18  *
RADIUS:  Vendor, Cisco       [26]  26
RADIUS:   ssg-service-info   [251] 20  "Npp-tariff-sw-time"
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  Vendor, Cisco       [26]  13
RADIUS:   ssg-control-info   [253] 7   "QT679"
RADIUS:  Vendor, Cisco       [26]  15
RADIUS:   ssg-control-info   [253] 9   "QV33766"
RADIUS:  Vendor, Cisco       [26]  26
RADIUS:   ssg-control-info   [253] 20  "QB19712;1113489875"
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  NAS-Port            [5]   6   0
RADIUS:  NAS-Port-Id         [87]  13  "3/0/0/0.201"
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.10.100.7
RADIUS:  Acct-Session-Id     [44]  10  "000002D2"
RADIUS:  Event-Timestamp     [55]  6   1113490110
```

The dual quota functionality on the ISG can be deployed in combination with other specific prepaid functionality such as prepaid idle-timeout functionality and the volume threshold functionality. But as described in the "ISG Dual Quota Prepaid Service" section on page 71, the QT attribute is interpreted in combination with volume quota as a monitor timer and not a type of quota. The set of actions that the ISG takes when the billing server sends a specific set of values in its authorization response together with an idle timer are slightly different than on the SSG.

The most noticeable conditions are:

QT = 0

QX>0;>0 or 0;>0 or 0 - IT>0 or 0

On the SSG, the prepaid service would be disconnected on these conditions. On the ISG, the service will not be disconnected under these conditions because the QT parameter used in a dual quota service is a timer on the ISG to poll the billing server again for quota. Attributing the value 0 to the QT in an authorization response indicates to the ISG that it needs to turn off the time monitor functionality (see "ISG Dual Quota Prepaid Service" section for more information).

Table 8 shows the different set of actions that the ISG can take when the billing server sends a specific set of values in its authorization response, together with an idle-timeout value.

Table 8 ISG Tariff Switching Attribute Values and Actions

QT	QX, tariff switching, preswitch (PRE), postswitch (POST)	Idle Timeout	ISG Action
0	>0;0;0	0	ISG opens the traffic class session. Reauthorization occurs when user traffic starts.
0	>0;0;0	>0	ISG opens the traffic class session, but blocks user traffic (drops or redirects it). Reauthorization occurs after a time interval equal to that set for the idle timeout.
>0	>0;>0;>0	>0	ISG opens the traffic class session. Reauthorization occurs when QT or PRE is consumed before tariff switching, or when PRE and POST are consumed, or no user traffic starts for a time interval equal to that set for the idle timeout.
>0	>0;>0;0	>0	ISG opens the traffic class session. Reauthorization occurs when QT or PRE is consumed before tariff switching, or when tariff switching occurs, or no user traffic starts for a time interval equal to that set for the idle timeout.
>0	>0;>0;>0	0	ISG opens the traffic class session. Reauthorization occurs when QT or PRE is consumed before tariff switching, or when PRE and POST are consumed.
>0	>0;>0;0	0	ISG opens the traffic class session. Reauthorization occurs when QT or PRE is consumed before tariff switching, or when tariff switching occurs
>0	>0;0;0	0	ISG opens the traffic class session. Reauthorization occurs when QT is consumed, or when user traffic starts.

Additional References

This section provides the following additional reference information:

Related Documents

Related Topic	Document Title
SESM installation and configuration	*Cisco Subscriber Edge Services Manager Installation Guide*
ISG configuration	*Cisco IOS Intelligent Service Gateway Configuration Guide* Cisco IOS ISG Command Reference
SSG configuration	*SSG Configuration Guide*

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Appendix

This appendix contains the following supplementary information:

SSG-to-ISG Migration Caveats and Workarounds

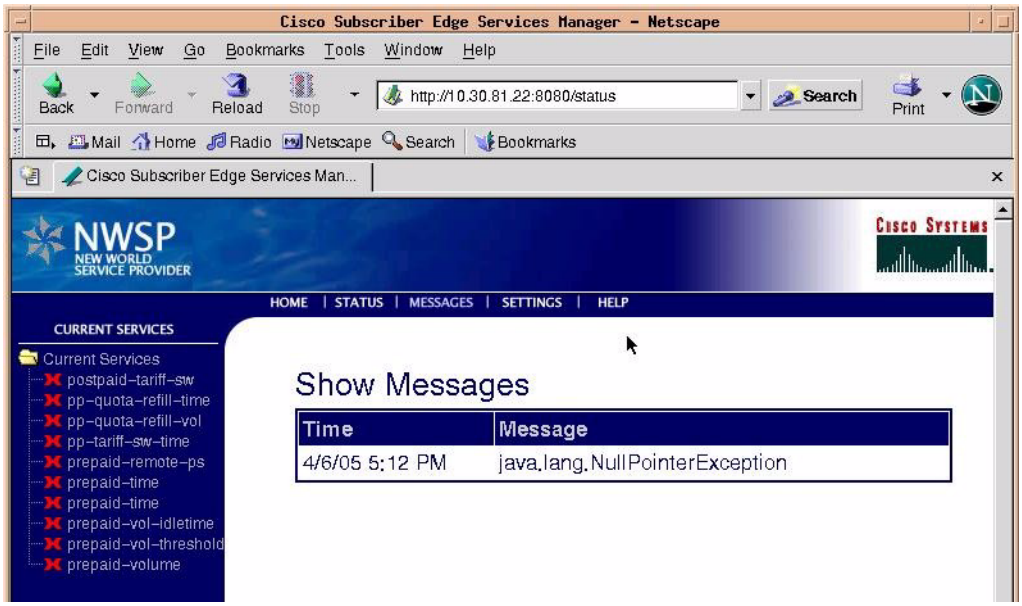
This section provides the following problem reports and workarounds from the team at Cisco Systems testing the SSG-to-ISG migration:

CSCuk56681—ISG Sending Locally Defined Service to Portal Breaks Status Page

When the ISG has locally defined services in the configuration, and these local services are applied to a user session, the ISG sends the Account-Info N attribute to the SESM service selection web page, to indicate that the named service is active. The locally defined services on the ISG are also sent over to the SESM service selection web page when SESM is doing an account query, to verify the status of the services the subscriber is currently using. SESM will poll the RADIUS server to know more about these active services, but because they only exist on the ISG, SESM will not receive any information from the RADIUS server about these services.

This is not a problem unless you need to verify the status of all active services. Figure 4 shows a sample SESM service selection web page with a link status that reflects the status of all active services. However, clicking the status link displays an error message.

Figure 4 SESM Service Selection Web Page with Status Error Message

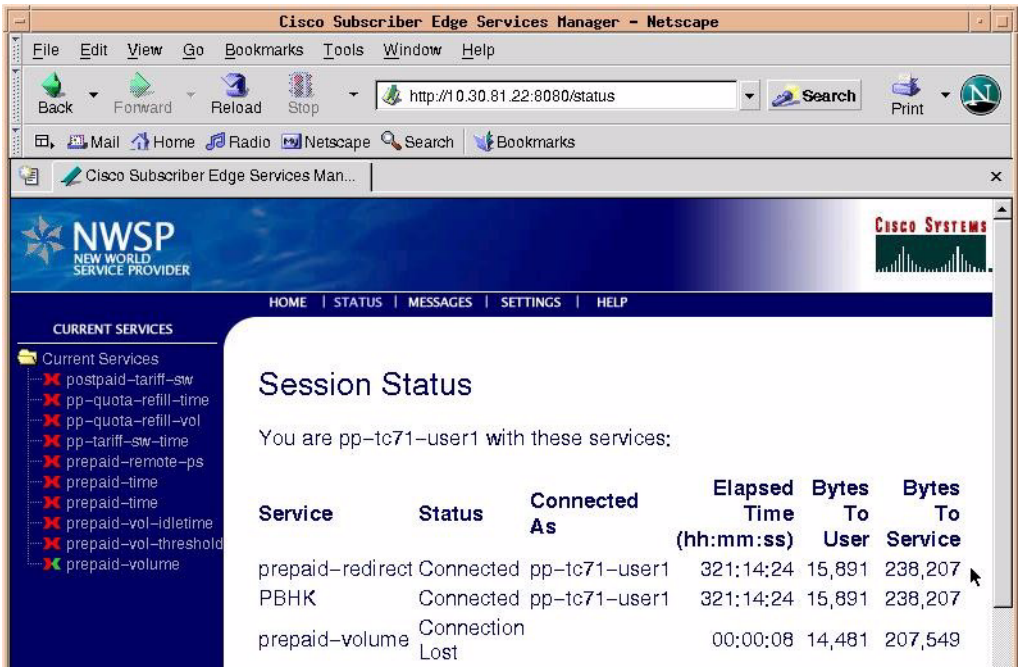


Because the service is defined locally on the ISG, and because the ISG sent the service selection web page the Account-Info N attribute, the portal will attempt to download the service profile from AAA each time you click the status page, and fail.

This failure occurs because SESM did not receive any answer from the RADIUS server about these services. To overcome this problem, you could insert the names of these local services on your RADIUS server, taking care not to define any Service-Info attributes for these services that would become selectable on your SESM service selection web page. A simple RADIUS profile containing the name of the local services—for example, ip_portbundle_service and l4_redirect_service, and a password for the profile—is all that is needed.

Figure 5 shows the status page once this fix is implemented.

Figure 5 SESM Service Selection Web Page with Simple Profile Fix



If the information in this display could be confusing for subscribers, use the Service-Info I attribute to inform subscribers that they need not be concerned with this display.

CSCeg56118—ISG Sends Different Error Code than SSG for Proxy Service Activation Failure

In a situation where proxy service activation fails because a subscriber submitted an incorrect username or password while using an SSG, an error message is displayed and the subscriber is required to enter the username and password again. In the same situation, however, the ISG sends a different error code than the SSG.

CSCeh03451—Periodic Accounting on Flows Behaves Inconsistently in the ISG

Periodic accounting in AAA can be enabled using the **aaa accounting update interval 500** command (the **interval** value is entered in seconds). This command enables periodic accounting on every session and flow that has accounting enabled. If you want to avoid this activity and enable periodic accounting on only individual sessions, use the **no aaa accounting update interval 500** command to disable periodic accounting on every session and flow, and configure RADIUS attribute 85 for per-user periodic accounting. However, the following notes apply to use of RADIUS attribute 85:

- Attribute 85 works only for PPP sessions in the user profile. If the attribute is present in a user profile for IP sessions, it will not be processed.
- Attribute 85 can be present in a service profile to signify that periodic accounting needs to be enabled only for the flow, but this is not currently the way it works.
- In the **policy-map service** command configured on the ISG, there is no keyword to configure periodic accounting in the service profile. This missing functionality is inconsistent. Because it is possible to configure periodic accounting inside RADIUS profiles, it should also be possible to configure it in local service profiles.

CSCeh35036—Two Traffic Classes with L4 Redirect Do Not Work

Two traffic classes on which prioritization and L4 redirection are applied, and for which the ACLs used to do the traffic classification overlap, cannot be used at the same time by the same subscriber. If there is an attempt to use these features at the same time, return traffic will fail to get translated again when it is translated using the traffic class service that was last applied.

CSCsa86854—Log Function on ACL Breaks Traffic Classification

When logging is enabled on an extended ACL, and the ACL is used to classify packets on an ISG, all traffic matching the ACL is incorrectly dropped. When the **log** keyword is removed from the extended **access-list** command, everything works as expected.

ISG Network Configuration Example

The following partial example shows a typical configuration for an ISG:

```
.
.
.
aaa new-model
!
!
aaa group server radius SERVER_GROUP
server 10.0.0.3 auth-port 1645 acct-port 1646
!
aaa group server radius proxy-rsim
server 10.0.0.10 auth-port 1812 acct-port 1813
!
aaa authentication login default none
aaa authentication login WEB-LOGIN group SERVER_GROUP
aaa authentication login proxy-rsim group proxy-rsim
aaa authentication ppp default group SERVER_GROUP
aaa authorization network default group SERVER_GROUP
aaa authorization subscriber-service default local group SERVER_GROUP
aaa accounting network default start-stop group SERVER_GROUP
aaa server radius sesm
 client 10.0.0.1
 key cisco
 port 1812
 message-authenticator ignore
!
!
aaa session-id common
ip subnet-zero
!
!
ip ftp username root
ip ftp password apasswd
no ip dhcp use vrf connected
!
!
ip vrf VPN301
rd 1000:301
route-target export 1000:301
route-target import 1000:301
!
ip cef
!
```

```
subscriber feature prepaid default
  threshold time 0 seconds
  threshold volume 1000 bytes
  method-list author default
  method-list accounting default
  password apasswd
!
subscriber policy recording rules limit 64
redirect server-group redirect-group
  server ip 10.0.0.1 port 8090
!
no mpls traffic-eng auto-bw timers frequency 0 call rsvp-sync
!
!
!
!
!
class-map type traffic match-any traffic_class_default_network
  match access-group input 110
  match  access-group output 111
!
class-map type traffic match-any L4redirect-tc-example
  match access-group output name redirect-acl
  match  access-group input name redirect-acl
!
class-map type control match-any service2-check
  match service-name group3-service2
!
class-map type control match-any service1-check
  match service-name group3-service1
  match service-name group3-service3
  match service-name group3-service4
!
class-map type control match-any test
!

policy-map type service example_network
class type traffic traffic_class_default_network
class type traffic default in-out
    drop

policy-map type service ip_portbundle
ip portbundle

policy-map type service l4_redirect
10 class type traffic L4redirect-tc-example
   redirect list 199 to group redirect-group
!
policy-map type control example-map1
class type control service1-check event service-start
 1 service-policy type service identifier service-name
!
class type control service2-check event service-start
 1 service-policy type service identifier service-name
 2 service-policy type service aaa list default name group3-service2
!
class type control always event session-start
 1 service-policy type service name example_network_service
 2 service-policy type service name ip_portbundle
 3 service-policy type service name l4_redirect
!
class type control always event service-stop
 1 service-policy type service unapply identifier service-name
!
```

```
!
!
bba-group pppoe GROUP3
virtual-template 1
!
!
vc-class atm VC_GROUP3
 protocol pppoe group GROUP3
 encapsulation aal5snap
!
interface Loopback0
ip address 10.10.10.3 255.255.255.255
!
interface Loopback1
ip address 192.168.21.1 255.255.255.0
!
interface Vif1
no ip address
!
interface FastEthernet0/0
ip address 192.168.3.1 255.255.255.0
ip portbundle outside
duplex auto
speed auto
mpls mtu 1522
!
interface FastEthernet0/1
ip address 10.10.20.3 255.255.255.0
duplex auto
speed auto
!
interface ATM1/0
no ip address
no atm ilmi-keepalive
no atm enable-ilmi-trap
bundle-enable
!
interface ATM1/0.301 point-to-point
ip address 192.168.12.1 255.255.255.0
atm route-bridged ip
no atm enable-ilmi-trap
pvc 1/301
 class-vc VC_GROUP3
!
!
interface ATM1/0.302 point-to-point
no atm enable-ilmi-trap
pvc 1/302
 class-vc VC_GROUP3
!
!
interface Virtual-Template1
ip unnumbered Loopback1
no keepalive
ppp authentication chap
ppp timeout aaa
service-policy type control example-map1
!
interface Virtual-TokenRing1
no ip address
ring-speed 16
!
router ospf 100
router-id 10.10.10.3
```

```
log-adjacency-changes
redistribute connected subnets route-map connected-to-ospf
redistribute static subnets network 10.10.10.3 0.0.0.0 area 300 network 192.168.3.0
0.0.0.255 area 300 distribute-list deny-ospf-external-routes in !
router bgp 1000
no synchronization
bgp router-id 10.10.10.3
bgp log-neighbor-changes
neighbor 10.10.10.101 remote-as 1000
neighbor 10.10.10.101 update-source Loopback0 no auto-summary
!
address-family vpnv4
neighbor 10.10.10.101 activate
neighbor 10.10.10.101 send-community both exit-address-family
!
address-family ipv4 vrf VPN301
redistribute connected
no auto-summary
no synchronization
exit-address-family
!
ip local pool POOL_GROUP3 192.168.21.100 192.168.21.200
ip local pool migration-lab-group3 10.10.3.1 10.10.3.14
!
ip portbundle
match access-list 110
source Loopback0
!
ip classless
ip route 10.10.3.0 255.255.255.0 Null0
ip route 10.10.0.0 255.255.255.0 10.10.20.104
!
no ip http server
!
!
!
ip access-list standard connected-to-ospf permit 192.168.0.0 0.255.255.255
ip access-list standard deny-ospf-external-routes permit 10.10.10.101 permit 10.0.0.0
0.0.0.255
!
ip access-list extended redirect-acl permit tcp any any eq www
ip radius source-interface Loopback0
access-list 55 permit 10.10.0.11
access-list 56 permit 10.10.0.12
access-list 57 permit 10.10.0.13
access-list 58 permit 10.10.0.14
access-list 110 permit ip any 10.0.0.0 0.0.0.255
access-list 111 permit ip 10.0.0.0 0.0.0.255 any
access-list 155 permit ip any host 10.10.0.11
access-list 156 permit ip any host 10.10.0.12
access-list 157 permit ip any host 10.10.0.13
access-list 158 permit ip any host 10.10.0.14
access-list 199 deny   tcp any host 10.0.0.1 eq www
access-list 199 deny   tcp any host 10.0.0.1 eq 8080
access-list 199 deny   tcp host 10.0.0.1 any
access-list 199 permit tcp any any eq www !
route-map connected-to-ospf permit 10
match ip address connected-to-ospf
!
!
radius-server attribute 44 include-in-access-req
radius-server attribute 55 include-in-acct-req
radius-server host 10.0.0.3 auth-port 1645 acct-port 1646 key cisco
radius-server host 10.0.0.10 auth-port 1812 acct-port 1813 key ww
```

```
radius-server vsa send accounting
radius-server vsa send authentication
!
control-plane
!
!
dial-peer cor custom
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
exec-timeout 0 0
logging synchronous
!
!
end
```

Glossary

AAA—authentication, authorization, and accounting.

ACL—access control list.

AV pair—attribute-value pair.

CoA—Change of Authorization.

CPE—customer premises equipment.

DHCP—Dynamic Host Configuration Protocol.

DNS—Domain Name System.

ISG—Intelligent Service Selection Gateway.

L2TP—Layer 2 Tunnel Protocol

L4—Layer 4.

LNS—Layer 2 network server.

MPLS—Multiprotocol Label Switching.

MTU—maximum transmission unit.

PBHK—Port-Bundle Host Key.

ping—packet internet groper.

PPP—Point-to-Point Protocol.

PPPoE—PPP over Ethernet.

QoS—quality of service.

RPC—remote procedure call.

SESM—Subscriber Edge Services Manager.

SMTP—Simple Mail Transport Protocol.

SSG—Service Selection Gateway.

SSO—Single Sign-On.

UDP—User Datagram Protocol.

URL—uniform resource locator.

VPDN—virtual private dialup network.

VRF—VPN routing and forwarding instance.

VSA—vendor-specific attribute.

Note See *Internetworking Terms and Acronyms* for terms not included in this glossary.