Cisco Service Control Mobile Solution Guide

Release 3.7.x

May 20, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-24167-04

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Service Control Mobile Solution Guide

CONTENTS

About this Guide

Revised: May 20, 2013, OL-24167-04

Introduction

This preface describes who should read the *Cisco Service Control Mobile Solution Guide*, how it is organized, and its document conventions.

This guide is for experienced network administrators who are responsible for configuring and maintaining the Cisco Service Control solution in a mobile environment.

Document Revision History

Table 1 records changes to this document.

Table 1 Document Revision History

Revision	Cisco Service Control Release and Date	Change Summary
OL-24167-04	Release 3.7.x May 20, 2013	Updated, Chapter 2, "Diameter Interface Support."
OL-24167-04	Release 3.7.x August 21, 2012	Updated, Chapter 3, "Gx Interface Support."
OL-24167-04	Release 3.7.x August 16, 2012	Updated, Chapter 2, "Diameter Interface Support."
OL-24167-04	Release 3.7.x July 24, 2012	Updated, Appendix A "Supported Message Formats."
OL-24167-04	Release 3.7.x March 29, 2012	Improved the quality of the user documentation by adding customer and internal feedback.
OL-24167-03	Release 3.7.x January 06, 2012	Updated with information pertaining to Release 3.7.2. • Updated the Table 6-3 with details about four new subscriber attributes. • Updated the example pertaining to the **show sub-attribute dictionary** command output. • Updated the list of supported VSAs in Table B-1.
OL-24167-02	Release 3.7.x October 25, 2011	Improved the quality of the user documentation by adding customer and internal feedback.
OL-24167-01	Release 3.7.x June 13, 2011	First version of the document.

Organization

This guide contains the following sections:

Table 2 Document Organization

Section	Title	Description
1	Introduction to the Cisco Service Control Mobile Solution, page 1-1	Provides an overview of the components of the Cisco Service Control Mobile solution.
2	Diameter Interface Support, page 2-1	Explains how to configure and monitor the diameter interface.
3	Gx Interface Support, page 3-1	Explains how the Gx interface works and how to configure it.
4	Gy Interface Support, page 4-1	Explains how the Gy interface works and how to configure it.
5	Gx RLS9 Interface Support, page 5-1	Explains the Gx RLS9 usage-monitoring capabilities and how to configure usage monitoring.
6	Capturing and Reporting Subscriber Attributes, page 6-1	Explains the various methods for capturing subscriber attributes. Explains how to include subscriber attributes in SCA BB reports, and presents samples of some Mobile reports.
A	Supported Message Formats, page A-1	Provides a detailed explanation of message formats for all interfaces.
B	Supported VSAs, page B-1	Provides a list of supported VSAs.

Related Publications

Your SCE platform and the software running on it contain extensive features and functionality, which are documented in the following resources:

- For further information about the Service Control CLI and a complete listing of all CLI commands, see the *Cisco SCE 8000 CLI Command Reference*
- For further information about configuring the SCE platform, see the relevant guide:
  - *Cisco SCE 8000 10GBE Software Configuration Guide*
  - *Cisco SCE 8000 GBE Software Configuration Guide*
- For further information about configuring the SCA BB application, see the *Cisco Service Control Application for Broadband User Guide*
- For viewing Cisco documentation or obtaining general information about the documentation, see the following sources:
  - *Obtaining Documentation and Submitting a Service Request, page xii*
  - The Cisco Information Packet that is shipped with your Cisco SCE 8000 platform.

Conventions

This document uses the following conventions:

Table 3 Conventions

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem*.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning **Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.**

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

Introduction to the Cisco Service Control Mobile Solution

Revised: March 29, 2012, OL-24167-04

General Overview

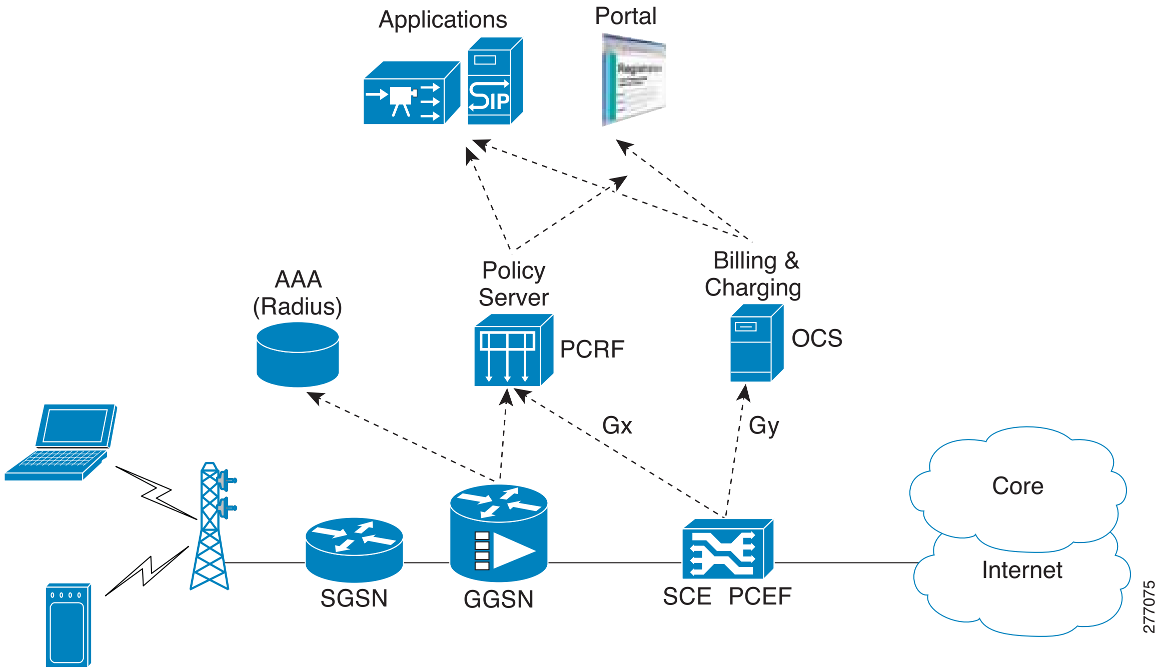
This document introduces the Service Control Application for Broadband (SCA BB) Release 3.7.0 mobile solution.

As a part of the Cisco Service Control mobile solution, Cisco SCA BB 3.7.0 supports the following reference points:

- Gx reference point for policy provisioning as described in Third Generation Partnership Project (3GPP) TS 29.212 V7.2.0
- Ro reference point (Gy interface) for online charging as described in 3GPP TS 32.299 V6.6.0.

Figure 1-1 depicts the topology of the Cisco Service Control mobile solution with respect to the Gx and Ro reference points.

Figure 1-1 Cisco Service Control Mobile Solution Topology



Diameter Stack Introduction

The SCA BB diameter stack serves the Gx and Gy interfaces. The infrastructure includes:

- Handling of transport layer connections
- Peer table
- Routing table
- Forwarding Scheme table (used to define the Load Balancing (LB) and High Availability (HA) configurations.)
- Error handling at the diameter level (used to send watch dog messages (keep alive), restart connections on failure, and so on.)

Gx Interface Introduction

The Gx interface is used to connect between the Policy and Charging Rules Function (PCRF) server and the Service Control Engine (SCE). Subscriber parameters, both SCE-specific (for example, package ID), and non-SCE-specific parameters, known as RADIUS Vendor Specific Attributes (VSAs), can be configured to the SCE through the Gx interface. The subscriber parameter update can be triggered both by SCE events, such as login and logout, and by PCRF external events.

Gx interface can also be used as an additional subscriber integration method. When using the Gx interface as a subscriber integration method, the PCRF provides the subscriber name in addition to the subscriber parameters.

Gy Interface Introduction

The SCA BB works with the Gy protocol interface in addition to working with SCE-propriety protocol for external quota management. The external quota management support is based on the current Cisco SCA BB Quota Manager support.

For additional information on the Gy interface, see Gy Interface Support, page 4-1.

Gx RLS9 Interface Introduction

The Gx RLS9 interface uses only the Gx interface to provide support for:

- Fair usage at bearer level—Requires reporting usage volume per subscriber session.
- Fair usage at flow level—Requires reporting usage volume per subscriber flow.

Note Gx RLS9 support is in accordance with 3GPP TS 29.212 V9.1.0, but is not in full compliance with this standard.

Combination of Subscriber Management Methods

The SCE supports combining various interfaces for subscriber management and reporting:

- Subscriber management can be done by either the Subscriber Manager (SM), or by PCRF (Gx), or using a combination (SM for login and VSA, Gx for subscriber package and VSA).

  In general, the entire SCE platform must be configured to work for all subscribers in the same way. For example, the system does not work if the Gx manages some of the subscribers and SM manages some of the subscribers. However, when the Gx interface is used for subscriber management, some of the subscribers can use Gy charging and others can use Gx RLS9. This is accomplished by configuring different packages for each charging interface, so that the internal mechanisms work the same for all subscribers.

- Subscriber reporting or charging can be over either Raw Data Records (RDR), Gy, or Gx RLS9.

  Reporting using RDR is always supported in parallel with Gy and Gx RLS9, including reporting VSAs.

Virtualized Intelligent Pipes for All-IP Mobile Networks

In the rapidly changing mobile environment, mobile service providers are constantly facing new challenges:

- Mobile wireless networks are evolving from the hierarchical circuit-based architecture to a flattened all-IP architecture.
- Enhanced radio technologies now allow true broadband data services.
- The combination of increasing demand for high data rate and increasing complexity on the Base Station presents a challenge to manage this last over-the-air mile correctly.

As next-generation all-IP mobile networks face significant challenges in managing the rapid growth of data traffic, a new approach is required to control the user traffic effectively using a multidimensional mechanism.

The Cisco Service Control solution introduces the concept of Virtualized Intelligent Pipes (VIP). The VIP uses deep packet inspection and advanced flow control to provide network optimization in all-IP wireless networks. The VIP enables mobile service providers to enforce traffic control rules per subscriber, per application, and per access link at the subscriber edge of the network.

The VIP provides:

- Enhanced network optimization taking into account the key bottlenecks of next-generation mobile networks: base station and backhaul link
- Optimization of operational expenditures using a centralized management approach, compared to a fully distributed traffic control in the Radio Access Network
- Quality Of Experience because traffic control rules are subject to subscriber and application prioritization

The VIP mechanism allows a Service Control node to enforce traffic control rules on access links that are not directly connected to it. Unlike traditional modes where traffic control is applied on the physical or logical interfaces connected to the router or switch, the Service Control approach classifies traffic into a VIP on which traffic control is enforced. The VIP is created by defining a mapping between the access link characteristic and a virtual pipe; traffic control rules then associate user traffic to this virtual pipe. The bandwidth is controlled completely via virtual links, with no need to modify the policy of subscribers in a congested cell.

For example, consider a base station to VIP mapping. Radio Frequency (RF) planning assesses the capacity of each base station in terms of coverage, capacity, and bandwidth. The base station characteristics are derived from the geographical area type (urban, suburban, rural), available spectrum, interferences, link budget, and so on. In this example, several types of base stations are mapped to VIPs using an index for uplink and downlink traffic control. The VIP traffic control rules are defined in terms of Peak Information Rate (PIR) for uplink and downlink traffic. Table 1-1 lists the VIP index and PIR for each base station type.

Table 1-1 Base Station to VIP Mapping

Base Station Type	VIP Up/Down Index	Virtual Link Up/Down PIR
Urban	1 / 2	900/9000 Kbps
Suburban	11/12	600/6000 Kbps
Rural	21/ 22	400/4000 Kbps

You can use templates to define VIP control rules for base stations with similar capacity, as well as change PIR values during peak hour.s

Similarly, Cisco Service Control enables you to define different service plans for subscribers corresponding to bandwidth allowance (such as 2 Mbps down and 512 kbps up), time/volume allowance, and applications allowance (VoIP, VoD, P2P). You can also associate traffic control rules to these service plans, which are enforced on a per user basis.

The mapping of subscriber to IP address and to VIP can be easily achieved. Because, the base station identification is signaled over the control plane towards the Access Gateway (ASN-GW, GGSN), subscriber management entities (AAA, Policy Manager), and Service Control element. You can also be change this mapping dynamically using a policy control layer based on a defined trigger (such as mobility or time of the day).

Figure 1-2 VIP Concept

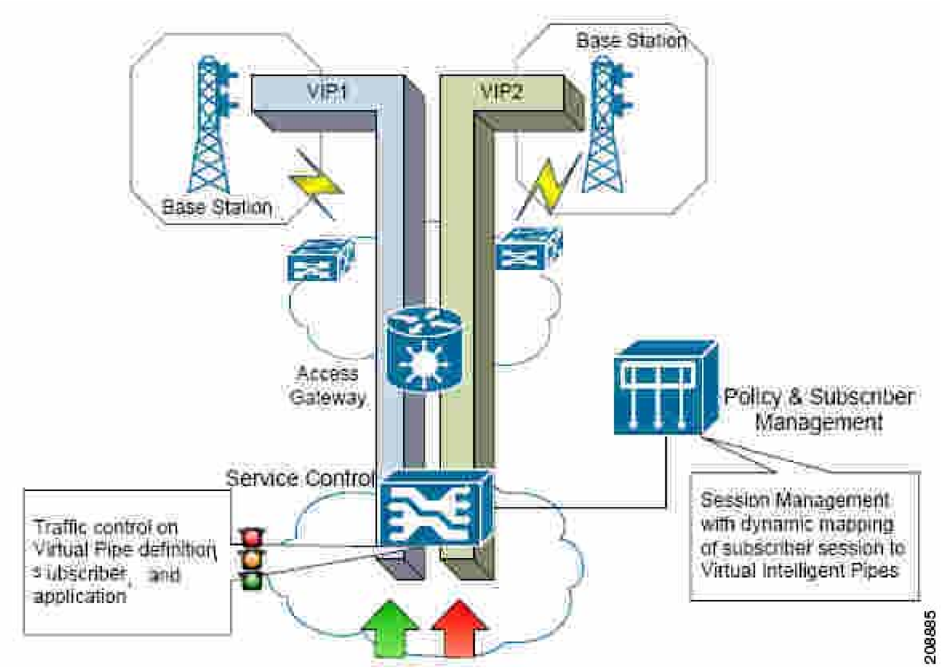

Base Station
VIP1
VIP2
Base Station
Access Gateway
Policy & Subscriber Management
Service Control
Traffic control on Virtual Pipe definition, subscriber, and application
Session Management with dynamic mapping of subscriber session to Virtual Intelligent Pipes
208885

Figure 1-2 shows the overall approach:

- Two VIPs (VIP1 and VIP2) are defined.
- The subscribers and traffic are mapped to the VIP using policy and subscriber management entities.
- You can classify the overall traffic into specific subscribers and applications, and enforce traffic control rules and the VIP control rule.

You can extend the approach described here to a cell-site backhaul link, multiple cell-sites, and so on.

CHAPTER 2

Diameter Interface Support

Revised: May 20, 2013, OL-24167-04

Overview

The diameter layer is responsible for maintaining connections to other diameter peers. This includes connecting to the peers, sending watch dogs (keep alive), and disconnecting from the peers.

The SCA BB diameter infrastructure includes several components: the standard diameter stack, the peer table, the routing table, and the forwarding scheme table, which defines the forwarding method for each realm. The supported forwarding methods are high availability (HA) and load balancing (LB).

The main entity in the diameter infrastructure is the peer table. The peer table includes all the peers that the SCE should connect to at the transport level. A Uniform Resource Identifier (URI) (usually ip:port) identifies each peer.

The routing table and the peer table support online configuration, that is, add and remove commands are supported while the diameter stack is up. The peer table and the routing table configurations are saved to the running configuration.

Peer State Machine

As shown in Figure A-2, after the establishment of a connection and successful exchange of Capability Exchange Request (CER) and Capability Exchange Answer (CEA) messages, the peers send watch dog messages. Even if a single watch dog message is not answered, the connection is disconnected and is considered down. The SCE tries to reestablish TCP connection once in every Tx timer time interval. When TCP connection is reestablished, the peer connection is still considered to be down until a Watch Dog Request (WDR) and a Watch Dog Answer (WDA) messages are exchanged.

Standard Diameter Stack

The standard diameter stack is used for sending and receiving diameter messages. The diameter stack supports both the Gx and Gy interfaces. There is only one diameter stack instance.

The diameter stack includes the following general configurations:

- Tx timeout
- Logging level
- Port
- Realm

The diameter stack holds general message statistics for non-application-specific messages.

The diameter stack includes start and stop operations. To prevent state loss, you cannot stop the stack while one of the interfaces is up.

Managing the Peer Table

The peer table lists all the peers with which the SCE has a direct connection. The information for each entry includes:

- Peer host—The host IP
- Peer port
- State—Nonconfigurable (Reflects the connection state (open or closed))

Table 2-1 lists the CLI commands used to configure and monitor the peer table.

Table 2-1 Peer Table CLI Commands

CLI Commands	Description
diameter peer <*name*> **peer-host** <*ip*> **port** <*port*>	Add entry to the peer table.
no diameter peer <*name*>	Remove entry from the peer table.
no diameter peer all	Clear the peer table.
show diameter peer-table	Show the peer table.
show diameter peer <*name*>	Show the specified peer table entry.

Example for adding a peer:

```
SCE8000(config)# diameter peer test_peer peer-host 1.1.1.1
```

Note Removing a peer from the peer table removes all the peer-related configuration information from the routing table and from the forwarding scheme table.

Example for executing a **show** command:

```
SCE8000> show diameter peer-table

Peer Table:
-------------------------------------------------------------
| Name            | Host                | Port     | State |
-------------------------------------------------------------
| SER_GX          | 10.121.64.38        | 3869     | Up    |
| SER_GY          | 10.121.64.46        | 3870     | Up    |
-------------------------------------------------------------
```

The Peer table lists the peers and their state. The state can be Up, Down, or N/A. N/A means the stack is not currently activated.

Note A peer is defined by a URI. Therefore, the same IP cannot be used on different ports to distinguish between two servers except when a domain name server (DNS) is used.

Managing the Routing Table

The routing table contains the peer application support and the forwarding scheme priority information. Each entry in the routing table includes the peer name, supported application, realm, and priority.

When the SCE sends an application message, it is sent to a realm and not to a specific server. In the Gx interface, there is one realm with many peers that support that realm. In the Gy interface, there can be several realms. Each peer can support both interfaces.

Table 2-2 lists the CLI commands used to configure and monitor the routing table.

Table 2-2 Routing Table CLI Commands

CLI Commands	Command Description
diameter realm <*realm name*> (Gx | Gy) peer <*name*> priority <*0-99*>	Add entry to the routing table.
no diameter realm <*realm name*> (Gx | Gy) peer <*name*>	Remove entry from the routing table.
no diameter realm <*realm name*> peer <*name*>	Remove all entries for the peer from the routing table.
no diameter realm all	Clear the routing table.
show diameter routing-table	Show the routing table.
show diameter realm <*realm name*>	Show all routing table entries that match the realm host.

Example for adding a route:

```
SCE8000(config)# diameter realm test_realm.cisco.com Gy peer test_peer priority 95
```

Example for showing the route table:

```
SCE8000> show diameter routing-table
 ---------------------------------------------------------
| Name        | Realm            | Application | Priority |
 ---------------------------------------------------------
| SER_GY      | cisco.com        | Gy          | 0        |
| SER_GX      | cisco.com        | Gx          | 0        |
 ---------------------------------------------------------
SCE8000>
```

In the example, the peer named SER_GY supports the Gy application on the cisco.com realm.

Diameter Load Balancing and High Availability Schemes

Diameter networks support load balancing (LB) and high availability (HA) schemes.

The diameter protocol sends messages to a realm and not to a specific server, letting other nodes in the diameter network take care of HA and LB schemes. Some diameter networks require that a network client handles the LB and HA. This is achieved by sending messages to a specific server that acts as the network client.

For information about load balancing and failover troubleshooting for the Gx interface, see the "High Availability for the Gx Interface" section on page 3-10. For information about load balancing and failover troubleshooting for the Gy interface, see the "Gy Interface Failover Support" section on page 4-22.

Forwarding Scheme Table

The Forwarding Scheme table defines the HA and LB scheme per each realm and application (one scheme per each combination of realm and application).

The following options are supported:

- LB with default HA
- HA with no LB

Table 2-3 lists the forwarding scheme examples for load balancing and high availability. For information on configuring the diameter forwarding scheme, see the "Diameter Forwarding Mode CLI Commands" section on page 2-8.

Table 2-3 Forwarding Scheme Examples

Model	Server	Load Balancing	High Availability
Load Balancing	A, B, C	Round Robin	When server A fails, the traffic is shared between server B and server C.
High Availability	A, B	None	Server A is primary. Server B is secondary.

Load Balancing

Load balancing is completed by round robin, using the available servers. The available servers are round robin cycled per session and not per message, that is, the messages for a specific session are all sent to the same server.

When a server fails, it is removed from the round robin.

If a server is removed from the round robin and a session has already initiated, an alternative server completes the session. The application can either start a new session or continue with the alternate server. For information on configuring the load balancing scheme, see the"Diameter Forwarding Mode CLI Commands" section on page 2-8.

High Availability (Failover)

When the high availability scheme is used, there is no load balancing between servers. The high availability scheme is strictly an active/standby scheme.

Each server is assigned a priority. Only the server with the highest priority handles the session. When the active server fails, all the new sessions are started on the next server in the priority list order. This mode supports stickiness, that is, when a failed server is back up, new sessions are forwarded to it, but already existing sessions remain forwarded to the secondary server unless transferred by an application decision. For information on configuring the high availability (failover) scheme, see the "Diameter Forwarding Mode CLI Commands" section on page 2-8.

Diameter Support Configuration

This section contains the information and instructions to configure and monitor the diameter forwarding, load balancing, and high availability schemes. This section contains the following subsections:

- Diameter Stack CLI Commands, page 2-7
- Diameter Forwarding Mode CLI Commands, page 2-8

Diameter Stack CLI Commands

Table 2-4 lists the CLI commands used to configure and monitor diameter stack support. All the commands, except **origin-realm** and **diameter port**, can be set while the stack is running.

Table 2-4 Diameter Stack CLI Commands

CLI Command	Command Description
[no] diameter	Start or stop the stack.
show diameter	Show the stack state.
show diameter counters	Show message statistics.
clear diameter counters	Reset all the statistics.
diameter origin-realm <*realm*>	Configure the stack realm. Run only when the stack is down.
diameter port <*port*>	Configure the stack host. Run only when the stack is down.
diameter logging-level <*level*>	Set the logging level of the stack.
diameter tx-timer <*timeout-in-seconds*>	Set the default timeout on the message.
default diameter origin-realm	Set origin-realm to default.
default diameter	Set stack state to default.
default diameter logging-level	Set stack logging level to default. Root-level command
default diameter tx-timer	Set tx timer to default.

Example for showing the diameter counters:

```
SCE8000> show diameter counters
WDR Sent     : 150
WDR Received : 182
WDA Sent     : 182
WDA Received : 150
CER Sent     : 3
CER Received : 0
CEA Sent     : 0
CEA Received : 3
DPR Sent     : 0
DPA Sent     : 1
```

Diameter Forwarding Mode CLI Commands

Table 2-5 lists the CLI commands used to configure and monitor the diameter forwarding mode.

Table 2-5 Diameter Forwarding Mode CLI Commands

CLI Command	Command Description
diameter realm <*realm*> (Gx | Gy) forwarding-mode (load-balancing | high-availability [shared-session-on [stickiness-on | stickiness-off] | shared-session-off])	Configure the forwarding mode. High availability mode has additional options: • shared-session-on – stickiness-on – stickiness-off • shared-session-off
show diameter forwarding-mode	Show load balancing and high availability configuration.

Example for configuring load balancing:

```
SCE8000(config)# diameter realm test_realm.cisco.com Gx forwarding-mode load-balancing
```

Example for configuring high availability:

```
SCE8000(config)# diameter realm realm test_realm.cisco.com Gy forwarding-mode
high-availability shared-session-on stickiness-off
```

CHAPTER 3

Gx Interface Support

Revised: August 21, 2012, OL-24167-04

Introduction

The Gx interface may be used for two purposes:

1. Setting the subscriber tunables (for example, package ID) and setting the subscriber RADIUS VSA attributes, which are used by the Gy interface.

   The subscriber parameters may be updated either by SCE or by PCRF triggering. SCE-initiated updates are mostly generated by login events, which result in sending CCR Initial/Update messages to the PCRF. PCRF can initiate an update by sending a RAR message to the SCE.

2. New subscriber integration method, where PCRF is responsible for coupling IP to the subscriber name in the SCE.

   Gx subscriber integration is used by setting Gx as anonymous-group manager (similar to SM pull mode).

Number of Subscriber IP Addresses Supported

The SCE supports a single IP address per subscriber when the Gx interface is used.

Gx Subscriber Properties and AVPs

The PCRF provides the Cisco SCE with the properties related to both Cisco SCA BB, and RADIUS VSA.

The properties that are related to the Cisco SCA BB and are provided by the PCRF to the Cisco SCE are:

- Package-id
- Real-time monitor
- Up virtual link
- Down virtual link

These properties are provided in the VSAs described in Table 3-1.

Vendor-Specific AVPs

Table 3-1 describes the vendor-specific Diameter AVPs defined for the Gx reference point. The Vendor-ID header of all the AVPs defined in this section is set to Cisco.

Table 3-1 Vendor-Specific AVPs

AVP Name	**AVP Code**	**Value Type**	**AVP Flag Rules**					
			Must	**May**	**Must Not**	**Should Not**	**May Encr.**	**Acc. Type**
Cisco-SCA BB-Package-Install	1000	Uint32	V	P		M	Y	All
Cisco-SCA BB-Real-time-monitor-Install	1001	Uint32	V	P		M	Y	All
Cisco-SCA BB-Vlink-Upstream-Install	1002	Uint32	V	P		M	Y	All
Cisco-SCA BB-Vlink-Downstream-Install	1003	Uint32	V	P		M	Y	All

Note The AVP header bit denoted as “M,” indicates whether support of the AVP is required. The AVP header bit denoted as “V,” indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see RFC 3588.

Cisco-SCA BB-Package-Install

- AVP code—1000
- Value type—Uint32
- Used to activate the SCE package as instructed by the PCRF. Defines the policy that will be assigned to the subscriber.
- Can be used either to install or to update the package ID to a subscriber.

Cisco-SCA BB-Real-time-monitor-Install AVP

- AVP code—1001
- Value type—Uint32
- Defines the SCE real-time monitor rule sent by the PCRF to the SCE. Activates and deactivates real-time monitoring for the subscriber.
  - Activate by sending a 1.
  - Deactivate by sending a 0.
  - Other values fail and are treated as error.

Cisco-SCA BB-Vlink-Upstream-Install AVP

- AVP—1002
- Value type—Uint32
- Defines the virtual link upstream rule sent by the PCRF to the SCE. Defines the upstream virtual link that the subscriber is assigned to. The virtual link is used to manage a group of subscribers that share a resource.
- Can be used either to install or update the virtual link upstream to a subscriber.

Cisco-SCA BB-Vlink-Downstream-Install AVP

- AVP—1003
- Value type—Uint32
- Defines the virtual link downstream rule sent by the PCRF to the SCE. Defines the downstream virtual link that the subscriber is assigned to.The virtual link is used to manage a group of subscribers sharing a resource.
- Can be used either to install or update virtual link downstream to a subscriber.

Gx Reused AVPs

Table 3-2 lists the Diameter AVPs reused by the Gx reference point from the existing Diameter applications. Other AVPs from the existing Diameter applications, except for the AVPs from the Diameter base protocol, do not need to be supported. The AVPs from the Diameter base protocol are not included in Table 3-2, but they are reused by the Gx reference point.

Where 3GPP RADIUS VSAs are reused, they are translated to Diameter AVPs, with the exception that the “M” flag is set and the “P” flag may be set.

Table 3-2 Gx Reused Diameter AVPs

Attribute Name	Description	Acc. Type
CC-Request-Number	Number of the request for mapping requests and answers.	All
CC-Request-Type	Type of the request (initial, update, termination).	All
Framed-IP-Address	IP version 4 (IPv4) address allocated to the subscriber.	All
Subscription-ID	Subscriber ID as defined in the PCRF, USER_E164.	All

Note See Appendix B, “Supported VSAs” for a complete list of supported VSAs.

Gx Session

The Gx session is the basic Gx entity and it is uniquely describes a subscriber and single IP mapping. The session is identified by a unique string (called session-id) and it is created both on the server and the SCE. Each Gx message must include the session-id AVP, which identifies the session that the message refers to.

Session Creation

The Gx session creation is initiated by the Cisco SCE. Session creation includes the exchange of Credit Control Request (CCR) and Credit Control Answer (CCA) messages. The Cisco SCE sends a CCR Initial message to the PCRF and the PCRF answers with a CCA message.

In the CCR Initial, the SCE sends the subscriber IP and subscriber name (if no Gx integration is used). The PCRF replies with a CCA Initial message, which includes a subset of the subscriber parameters. After the SCE receives a successful CCA Initial message (including a result AVP with success), the session is successfully opened. If the PCRF CCA Initial message includes error codes, the session is not created, and the Cisco SCE will attempt to reopen it later. However, the subscriber will be assigned to the anonymous group until the Cisco SCE receives a successful CCA initial message. For more details on the error handling of the CCA initial message, see the "Error Handling" section on page A-7.

Session Lifetime

During the lifetime of a Gx session, the following messages can be sent:

- CCR Update: Similar to CCR Initial, except that the session is already opened. The SCE asks the PCRF for updates on the parameters.
- RAR: Message sent from the PCRF to the SCE to update subscriber parameters. In this case, an external event causes the PCRF to update the subscriber parameters and send the updates to the SCE.

Session End

A session may be ended in either of two ways:

- The SCE may terminate the session by sending a CCR Terminate message. The CCR Terminate message is triggered by logout of the subscriber, either explicit (for example, SM logout) or implicit (by aging).
- PCRF may terminate the session by sending an Abort Session Request (ASR) message. The ASR message is intended to be used in Gx subscriber integration mode where an external event (for example, user disconnecting the mobile modem Internet connection) triggers the PCRF to close the session. The ASR terminates the session in both modes (Gx subscriber integration and other external integration methods). However, in Gx integration, the ASR also triggers a logout of the subscriber from the SCE.

Gx Session Life Cycle

The Gx session life cycle varies based on the whether or not the subscriber integration is external (set as none) or internal. The following sections describe the Gx session life cycles.

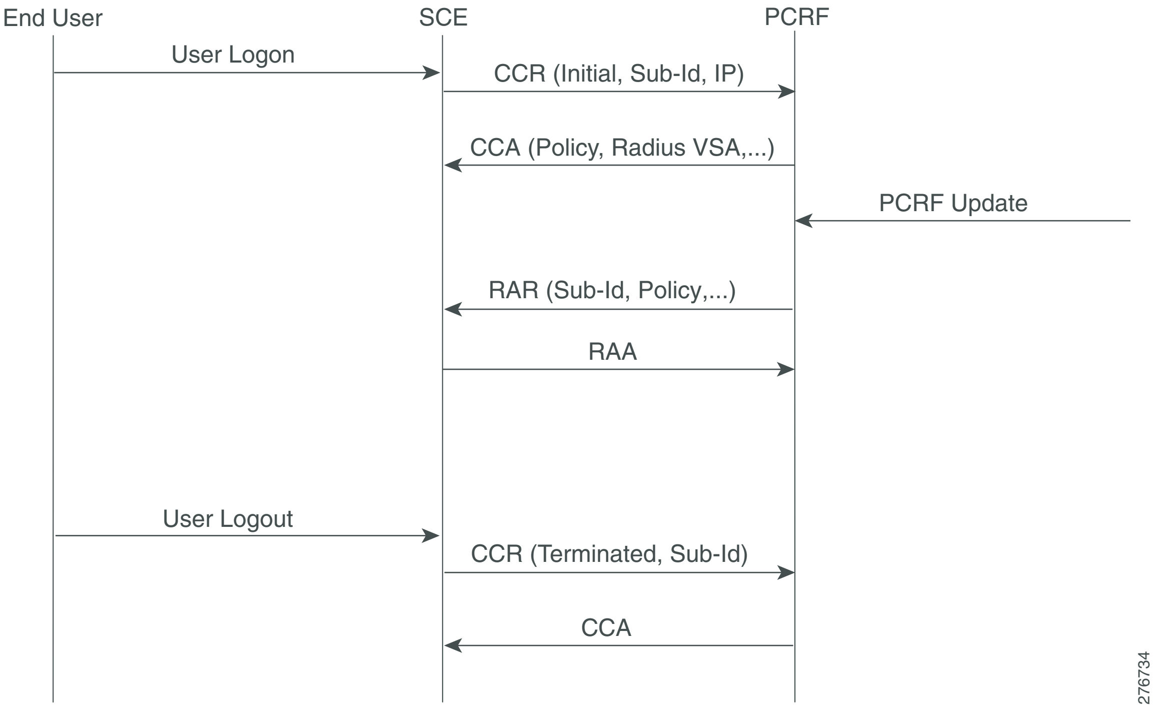
Gx Subscriber Integration (None)

In an external subscriber integration method such as SM, the Gx session is created when the subscriber logs in. The subscriber is logged in to the SCE by the external API (for example, SM). When the login process is complete, the SCE tries to open a Gx session for the subscriber and the IP tuple. After the session is created, (the PCRF responded with a successful CCA Initial), the subscriber parameters are extracted from the CCA message and updated. As described earlier, the PCRF may send a RAR message to the SCE during the life time of the session. CCR Updates may be sent to the PCRF as a result of the external API, such as SM sync.

The Gx session is terminated when the external API in use logs the subscriber out. The session can be terminated by sending an ASR message from the PCRF, although this does not trigger subscriber logout.

Figure 3-1 shows a typical flow of session messages. The flow starts when a subscriber is logged into the SCE, triggering a CCR and CCA message exchange. The session ends with user explicit logout, which terminates the session.

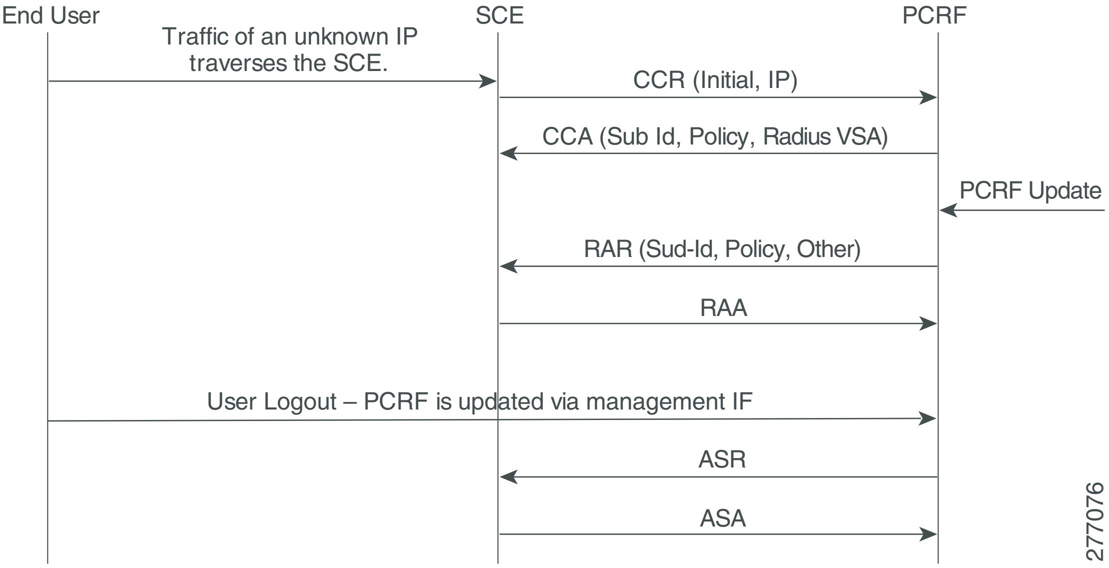
Figure 3-1 Gx Subscriber Integration (None) Flow



Gx Subscriber Integration

The Gx session life cycle is slightly different when Gx is the subscriber integration method. The Cisco SCE starts the Gx session upon identifying an anonymous IP that belongs to the Gx anonymous-group (similar to SM pull, where a pull notification is created). However, the Cisco SCE does not know the subscriber name, and therefore it is not sent as part of the CCR Initial message. The PCRF responds with a CCA Initial message that includes the subscriber name. The Cisco SCE logs in the subscriber, and sends the IP mapping to the Cisco SCE, together with the subscriber parameters. The Gx session may terminate in two ways, by aging, which generates subscriber logout, or by CCR Terminate, with the PCRF ending the session by sending an ASR. In the second scenario, the ASR also logs out the subscriber from the Cisco SCE because the Gx is the subscriber owner. See Figure 3-2.

Figure 3-2 Gx Anonymous-Group Flow


End User
SCE
PCRF
Traffic of an unknown IP traverses the SCE.
CCR (Initial, IP)
CCA (Sub Id, Policy, Radius VSA)
PCRF Update
RAR (Sud-Id, Policy, Other)
RAA
User Logout – PCRF is updated via management IF
ASR
ASA
277076

Whether the session is terminated by aging or by CCR Terminate, the PCRF may send a RAR in order to update the subscriber parameters.

Note Using Gx, the SCE supports single IP mapping per subscriber.

Configuring Gx Support

This section contains the information and instructions to configure and monitor the Gx support configuration.

Gx Interface CLI Commands

Table 3-3 lists the CLI commands used to configure and monitor the Gx interface.

Table 3-3 Gx Interface CLI Commands

CLI Command	Command Description
[no] diameter Gx	Start and stop Gx.
show diameter Gx	Show Gx state and connected peers.
show diameter Gx counters	Show Gx messages statistics.
clear diameter Gx counters	Reset Gx statistics.
diameter Gx tx-timer <*timeout-in-seconds*>	Set the time-out on messages. If the PCRF does not respond to a Gx message in the configured tx-timer seconds, the message is considered timed out. The message is dumped if it arrives after tx-timer expires.
diameter Gx PCRF-connection-failure-grace-time <*time*>	Set the Gx failover grace period. Failover functions as follows: • If a connection fails and is reestablished within the failover grace period, no failover action is taken. • If a connection fails and is not reestablished within the failover grace period, failover action is taken. • If a server fails, all its sessions remain open for the failover grace period. After the failover grace period expires, all the server sessions are closed and reopened on a secondary server. • If a server fails on a system using session-sharing, no failover action is taken.
diameter Gx fatal-grace-time <*time*>	Set the Gx detection timeout. If no connection to any server is detected for the configured length of time, all the diameter sessions are closed and a new connection is established.
[no]subscriber Gx-pull-request-disable	Stops the SCE from sending the subscriber pull request to the PCRF server.

Example for displaying the Gx configuration:

```
SCE8000> show diameter gx
Gx Application Status                          : Up
Gx Realm                                       : scos.com
Gx tx-timer                                    : 5
Gx PCRF-connection-failure-grace-time          : 150
Gx fatal-grace-time                            : 300
Connected
```

Example for enabling, disabling, and viewing the Gx pull request status:

```
SCE8000#> show interface LineCard 0 subscriber Gx-pull-request-disable
Gx-pull-request is enabled
SCE8000#> config
SCE8000(config)#> interface LineCard 0
SCE8000(config if)#> subscriber Gx-pull-request-disable
SCE8000(config if)#> show interface LineCard 0 subscriber Gx-pull-request-disable
Gx-pull-request is disabled
SCE8000(config if)#> no subscriber Gx-pull-request-disable
SCE8000(config if)#> show interface LineCard 0 subscriber Gx-pull-request-disable
Gx-pull-request is enabled
SCE8000(config if)#>
```

High Availability for the Gx Interface

Two parameters define the High Availability (HA) behavior:

- Session shared—Defines whether the session needs to reopen upon failover. When a shared session is defined, it is assumed that each session is common to all the servers (for example, through a common database).
- Stickiness—Defines whether the session needs to move back to the original server when it restarts.

A server is in failure mode if the underlying diameter connection fails and cannot recover for the configurable grace time. Fatal mode is when all the servers are in failure mode and no connections to PCRF exist.

Session not Shared with Stickiness

When the primary server fails, all the sessions managed by that server are migrated to the next server in a controlled manner (limited by the maximum rate allowed).

If the Gx session manages the subscriber, the subscriber is logged out. On the next traffic generating event, the subscriber logs in on a different server. If any other method manages the subscriber, only the Gx session is closed and the session reopens on the secondary server.

Eventually, all the subscribers relog and migrate to the secondary server. After the primary server is up, new sessions are forwarded to it. The migrated sessions on the secondary server continue on the secondary server until logout or failure.

In this scheme, a server failure causes a long convergence time.

In fatal mode, all the Gx-managed subscribers are logged out and all the other subscribers remain with their last configuration. When the connection resumes, the SCE reopens all the non-Gx-managed sessions and the Gx-managed sessions are triggered by traffic.

Example:

Servers A, B, and C with priority 100, 99, and 98, respectively.

1. After ten Gx sessions, all the servers are up and all the sessions are opened on server A. Servers B and C do not handle any sessions.
2. Servers A and B fail. The ten sessions are closed and are reopened on server C.
3. Server B is up. Server C continues to handle all its sessions, new sessions open on server B.
4. After nine more new Gx sessions, server A comes back up. Server A handles no sessions, server B handles nine sessions, and server C handles ten sessions.

Session Shared with Stickiness

In this scheme, the servers share the session. When the primary server is down, all the existing sessions are handled by the secondary server. No relogin is required.

When the primary server is up again, all the new sessions are handled by it, while old sessions that were moved to the secondary server remain on the secondary server until logout.

Fatal mode works in the same way as in a session not shared with stickiness.

Example:

Servers A, B, and C with priority 100, 99, and 98, respectively.

1. After 10 Gx sessions, all the servers are up and all the sessions are opened on server A. Servers B and C do not handle any sessions.
2. Servers A and B fail. The 10 sessions are handled by server C without being closed (no action is taken). When a message needs to be sent, it is sent to server C, and remains with server C until the session is closed.
3. Server B is up. Again no action is taken, all the messages related to the new sessions are sent to server B. Any messages related to the sessions handled by server C (Step 2) remain with server C.
4. After nine more new Gx sessions, server A comes back up. If a message was generated in Step 2 or 3 for a session, it remains with server B or server C, respectively. All the other messages are sent to server A.

Session Shared Without Stickiness

Same as the session shared with stickiness with the exception that when the primary server recovers, all the sessions are re-forwarded to it.

Fatal mode works in the same way as in a session shared with stickiness.

Example:

Servers A, B, and C with priority 100, 99, and 98, respectively.

1. After 10 Gx sessions, all servers are up, and all the sessions are opened on server A. Servers B and C do not handle any sessions.
2. Servers A and B fail. The 10 sessions are handled by server C without being closed (no action is taken). When a message needs to be sent, it is sent to server C.
3. Server B is up. No action is taken, all the messages are sent to server B.
4. After nine more new Gx sessions, server A comes back up. No action is taken, all the messages are forwarded to server A.

Load Balancing with Default High Availability

Load balancing is always done by round robin per available servers. Round robin is done per session and not per message, that is, all the messages for a specific session are sent to the same server.

When a server fails, it is removed from the round robin.

If a server is removed from the load balancing setup, sessions that are already initiated with that server will be closed. These sessions reopen on a new server and remain open with that server.

CHAPTER 4

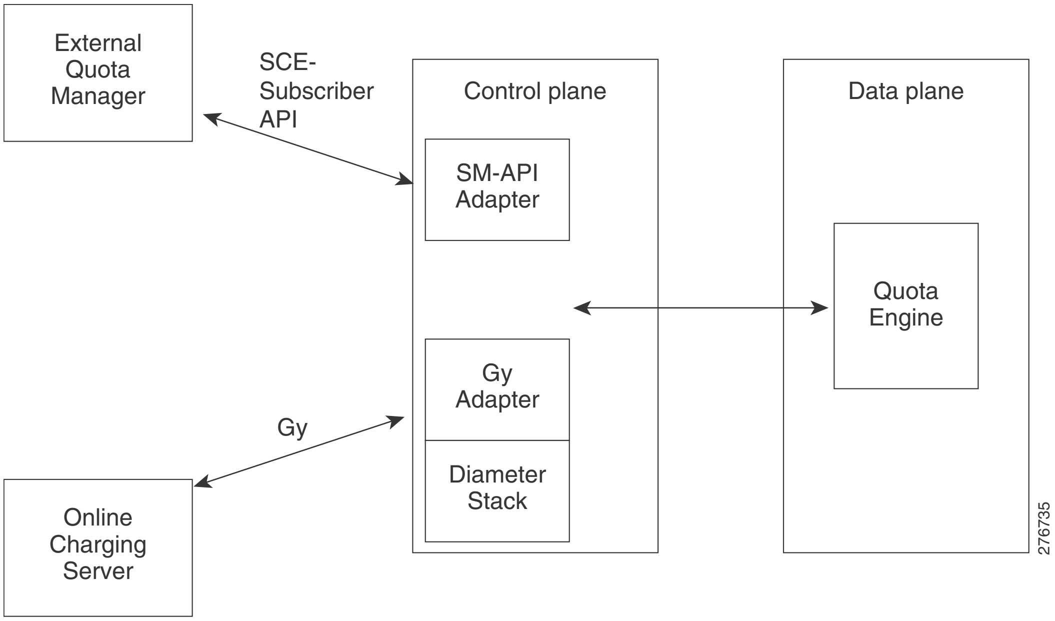
Gy Interface Support

Revised: March 29, 2012, OL-24167-04

Introduction

The Gy interface is used for reporting and charging. In SCA BB, support of the Gy interface is divided into two components. The two components reside on the control plane and the data plane, as shown in Figure 4-1.

Figure 4-1 Gy Interface Adapter



Gy Adapter (Control Plane)

The Gy adapter:

- Supports session charging with centralized unit determination and centralized rating
- Supports reauthorization by the online charging system (OCS)
  - Handles the failure handling of Diameter Credit-Control Application (DCCA) level errors and timeout messages according to the Credit-Control-Failure-Handling AVP
- Manages the HA and LB schemes
- Supports realm selection based on the 3GPP-Charging-Characteristics AVP
- Supports tariff change
- Supports quota threshold, validity time, quota holding time, and quota consumption time as described in 3GPP TS 32.299 and RFC 4006

SM-API Adapter (Control Plane)

The SM-API Adapter:

- Is backward compatible with existing APIs
- Supports 16 buckets in the same RDR
- Replaces tunable interface with user-handlers

Quota Engine (Data Plane)

The quota engine:

- Supports the centralized model and the decentralized model
- Supports 16 quota buckets as follows:
  - Supports time, events, and volume (total or inbound and outbound limitations)
  - Counts the consumed quota (pre-tariff and post-tariff change, if needed)
  - Supports quota validity time, threshold, and quota holding time (QHT)
  - Supports per-bucket, quota-exceeding action settings
  - Supports tariff change optimization
- Synchronizes quota in cascade mode (minimal data lost)

Gy Quota Model

The SCA BB supports three operational and integration quota management models that allow gradual investment and trade-off between complexity of integration/deployment and range of functionality:

- SCE Internal model—Time-based, autoreplenished quota
- SM Quota Management model—Time-based, autoreplenished quota with preserved state
- Flexible model—Integration with external quota manager. There are two types of external quota management—SM-API based, and Gy based.

The Gy quota model enables the Gy interface adapter to be used for the external quota management. The Gy quota model is based on session charging with central unit determination. An external OCS (for example, bucket type and post-breach action) controls the configuration of the quota buckets. In the Gy quota model, two subscribers from the same package can use different buckets, with different sizes and post-breach actions. In the Gy quota model, service association to buckets is completed using the SCA BB console. For additional configuration information using the SCA BB console, see the "Gy Interface Failover Support" section on page 4-22.

In the Gy type of quota management:

- All bucket types and quota limits are set to "Set externally"
- In the Usage Limit tab (in the Rule dialog box), only "external bucket" can be used
- An option is added to each bucket to declare whether to ask for quota upon login. By default, this option is set to false for all the buckets.

The Gy quota model supports the following quota types (with the related AVPs):

- Time—CC-Time
- Events—CC-Service-Specific
- Total volume—CC-Total-Octets
- Upstream volume—CC-Input-Octets
- Downstream volume—CC-Output-Octets
- Upstream_Downstream—CC-Input-Octets and CC-Output-Octets in separate Multiple-Services-Credit-Control (MSCC) AVPs

Note the following about the correspondence between buckets types, quota types, and AVPs:

- Each bucket can only be assigned or granted a single bucket unit type. Granting is done by providing a Granted-Service-Unit (GSU) AVP with the correct bucket type in the MSCC for the relevant bucket.
- For each bucket, a separate MSCC is used. The bucket ID must be unique in each MSCC.
  - An exception to this point is the UPSTREAM_DOWNSTREAM bucket type. This type accounts for the volume usage on the Downstream (CC-Output) and the Upstream (CC-Input) separately.

    To use this bucket type, the server should grant the client CC-Input GSU on a certain MSCC carrying the bucket ID and an additional separate grant of CC-Output GSU on a separate MSCC carrying the same bucket ID.
- Reports from the client are done similarly, but using the Used-Service-Unit (USU) AVP.

Quota Time

The quota time consumed is the service usage duration with either no idle time or minimum idle time. The quota time consumed is the quota consumption time (QCT). When the quota is granted, a QCT can be assigned. If QCT is not assigned, a default value per service is used.

Quota Volume

By default, the quota usage sampling frequency is set to 30 seconds and the sampling is completed once for every 32 packets assuming nontrivial activity. If the trivial activity exceeds the sampling time, the system charges per sampling unit. For example, in case of trivial activity of two minutes, the charging is 30 seconds.

When upstream-downstream volume is used, the debit is completed separately per upstream and downstream.

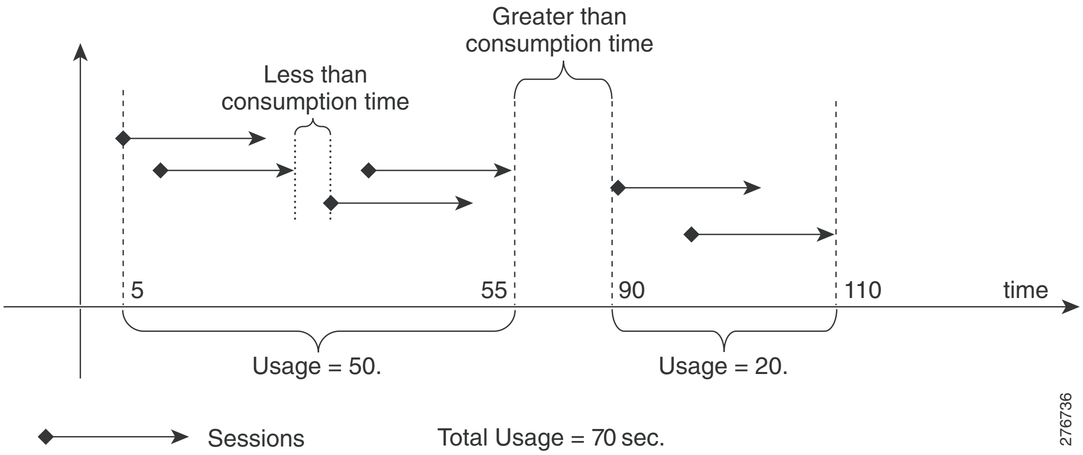
For additional Gy quota information, see the following sections:

- Time-Based Quota (Consumption Time), page 4-4
- Timers, page 4-5
- Quota Request, page 4-6
- Quota Threshold and Breach, page 4-7
- Tariff Time Change, page 4-7
- Gy Quota Threshold Call Flow, page 4-7

Time-Based Quota (Consumption Time)

The SCE defines time-based quota buckets and accounts for subscriber usage in seconds. The up and down volume and number of sessions are not critical in time-based quota management. The subscriber usage is accumulated as long as the subscriber has at least one active session. The server can specify a QCT for each bucket. The specified QCT is the maximum idle time that is accounted as quota usage. As shown in Figure 4-2, when the idle period is less than the consumption time, it is counted as subscriber usage, but when the idle period is greater than consumption time, it is not accounted for.

Figure 4-2 Quota Consumption Time



If the server fails to provide a consumption time, the SCE uses the default consumption time.

Timers

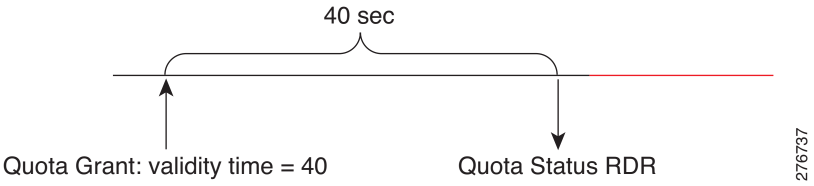
The supported quota timers are the Quota Validity Time and the Quota Holding Time.

- Quota Validity Time, page 4-5
- Quota Holding Time, page 4-5

Quota Validity Time

The server defines the quota validity time for each bucket. The time is measured in seconds. Quota validity time is the duration for which the SCE (or the subscriber) can use the quota as shown in Figure 4-3.

Figure 4-3 Quota Validity Time



If the server does not provide a quota validity time, the default validity time is used. The default validity time is defined per bucket per package in the GUI.

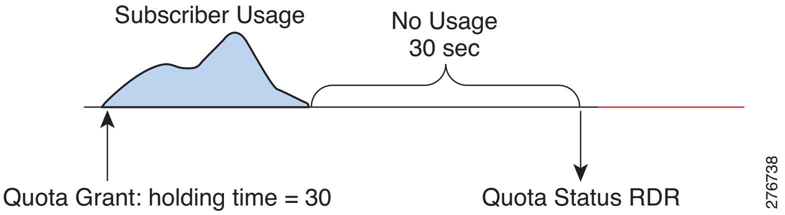
After the quota validity time expires, the SCE sends a Quota Status RDR and invalidates the bucket quota. It is the responsibility of the server to update the bucket quota and the action again. If the server does not respond, the bucket state is changed to error and an error action is applied to all the associated flows.

If the quota validity time expires, the Quota Status RDR is sent even if the server has specified Final Unit Indication.

Quota Holding Time

The server defines quota holding time, in seconds, for each bucket. Quota holding time indicates the duration for which the SCE can hold quota without any usage. The SCE resets the timer each time it detects subscriber activity on a flow that is associated with the bucket as shown in Figure 4-4.

Figure 4-4 Quota Holding Time



If the server does not provide a quota holding time, the default holding time is used. The default quota holding time is defined per bucket per package in the GUI.

After the quota holding timer expires, the SCE sends a Quota Status RDR and invalidates the bucket quota. The server is responsible to update the bucket quota and action again. If the server does not respond, the bucket state is changed to error and an error action is applied to all the associated flows.

If the quota holding timer expires, the Quota Status RDR is sent even if the server has specified Final Unit Indication.

Quota Request

A quota request is sent upon an attempt to use a service with no quota available, unless the service already received an indication that the quota is not available. For example, a quota request was sent, and the reply was “no quota available”.

If the service is marked to request quota upon login, quota requests are sent even before any attempt to use the service is executed. Quota requested upon login is configured per service package. The default is not to request quota upon login.

The quota count is started before the first grant. The only exceptions are short flows, which end before the quota is granted.

When a quota request occurs upon threshold, the quota is counted even after the quota request is sent. After the quota is granted, the already consumed quota is treated as consumed and subtracted from the granted quota.

If an external server is used to trigger a quota request, a quota reauthorization request should be used.

Quota Reauthorization Request

When the quota requires reauthorization, a debit request for the measured consumed quota (if it exists) is sent, asking for new quota. The response overrides the existing quota.

A reauthorization request is sent for the following events:

- Validity time expired
- Quota holding time (QHT) expired
- Threshold is reached
- Upon reauthorization request from the server
- Upon quota breach

The validity time and QHT may be provided with the quota grant. If the validity time and QHT are not specified, a default value is used. The default value is configured per bucket or package.

Quota Threshold and Breach

The quota threshold and breach actions are defined per quota. If quota threshold and breach are not specified, default values configured per service or package are used.

The supported quota threshold and breach actions are:

- Block
- Pass
- Redirect (uses Gy default notification)
- Use configured postbreach behavior as defined in the SCA BB console for the service

The actions may also include sending a predefined notification. The notification is predefined on the quota management table.

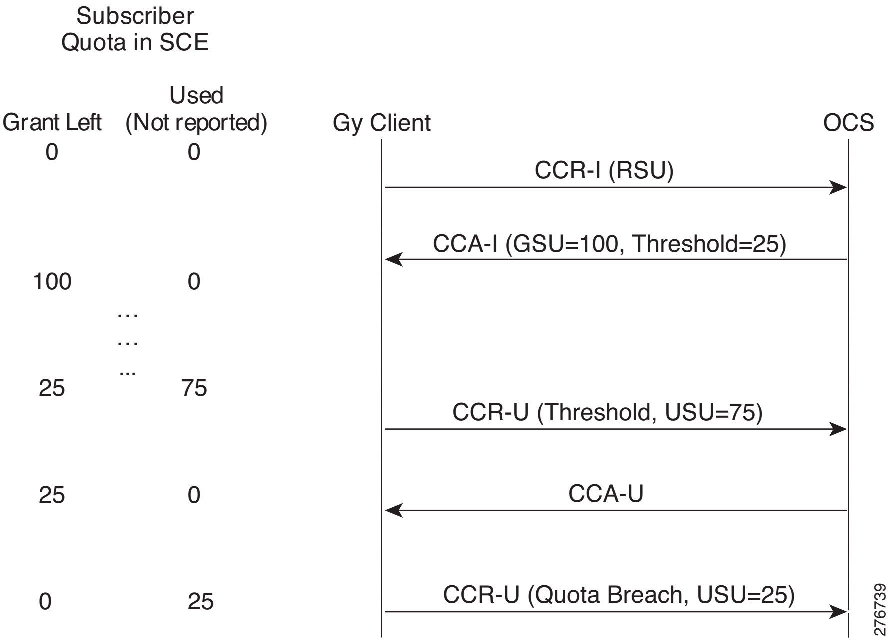
Tariff Time Change

Pretariff time change and post-tariff time change are reported in the quota debit request. The tariff change time is given per quota and is measured in number of seconds since 1.1.1900 (32 bits).

Gy Quota Threshold Call Flow

Figure 4-5 illustrates the Gy quota threshold call flow. The quota used report is reset only after the SCE receives the CCA-U message.

Figure 4-5 Gy Quota Threshold Call Flow



Gy Support Configuration

This section contains the information and instructions to configure and monitor the Gy support configuration and the Gy quota configuration.

Configuring Subscriber Attribute Mapping

You can map a specified PS Information AVP (3GPP-Charging-Characteristics) into a specified realm. Use the following CLI command:

diameter Gy subscriber-attribute-mapping attribute-name 3GPP-Charging-Characteristics attribute-value <*attribute-value*> **realm-id** <*realm-id*>

The realm selection is completed based on the subscriber RADIUS property 3GPP-charging-characteristics and the global mapping of potential realm values. If there is no mapping (or a mismatch), the first realm in the realm table is selected.

Note The Gx and Gy interfaces support 3GPP-charging-characteristics and it is assigned to a subscriber upon login via the Gx interface.

Gy Interface CLI Commands

Table 4-1 lists the CLI commands used to configure and monitor the Gy interface and Table 4-2 lists the CLI commands used to monitor the quota engine.

Table 4-1 Gy Interface CLI Commands

CLI Command	Command Description
[no] diameter Gy[1]	Enable the Gy application. **Note** Root-level command
show diameter Gy	Show the Gy state and the connected peers.
[default] diameter Gy tx-timeout <*timeout-in-seconds*>	Configure the Gy tx timeout value.
show diameter Gy (counters)	Show the Gy information and counters.
clear diameter Gy counters	Clear the Gy counters.
diameter Gy subscriber-attribute-mapping attribute-name 3GPP-charging-characteristics attribute-value <*attribute-value*> realm-id <*realm-id*>	Map the specified PS Information AVP (3GPP-Charging-Characteristics) into the specified realm.

[1] Upon disabling Gy, all the sessions are closed, and unreported quota is reported. New sessions do not open. When the Gy interface is on (again), new sessions are opened for all the subscribers.

Table 4-2 Quota Engine CLI Commands

CLI Command	Command Description
show interface LineCard 0 subscriber name <*name*> breach-state	Show all the breached buckets for the subscriber.
show interface LineCard 0 subscriber name <*name*> bucket-state	Show all the buckets used by the subscriber.
show interface LineCard 0 subscriber name <*name*> bucket-state id <*ID*>	Show the specific bucket size, usage, and state.

Configuring Gy Support (CLI)

To configure Gy support using the CLI, see the "Gy Interface CLI Commands" section on page 4-8.

Configuring Gy Support (GUI)

In the SCA BB GUI, you can create quota profiles that define the limits and action of each bucket and assign specific services to the bucket. You must attach the quota profile to a package and define a quota rule for the package for the relevant service.

Note For more information on configuring and managing quotas, see the *Cisco Service Control Application for Broadband User Guide*.

To configure a Gy quota profile, complete the following steps. The steps are described in detail in the referenced sections.

Step 1 Select Gy as the External Quota Type (Configuring the External Quota Type, page 4-11).

Step 2 Create the Gy Quota Profile (Adding a Quota Profile, page 4-13)

Step 3 Edit the buckets and assign services to the profile (Editing a Quota Profile, page 4-13).

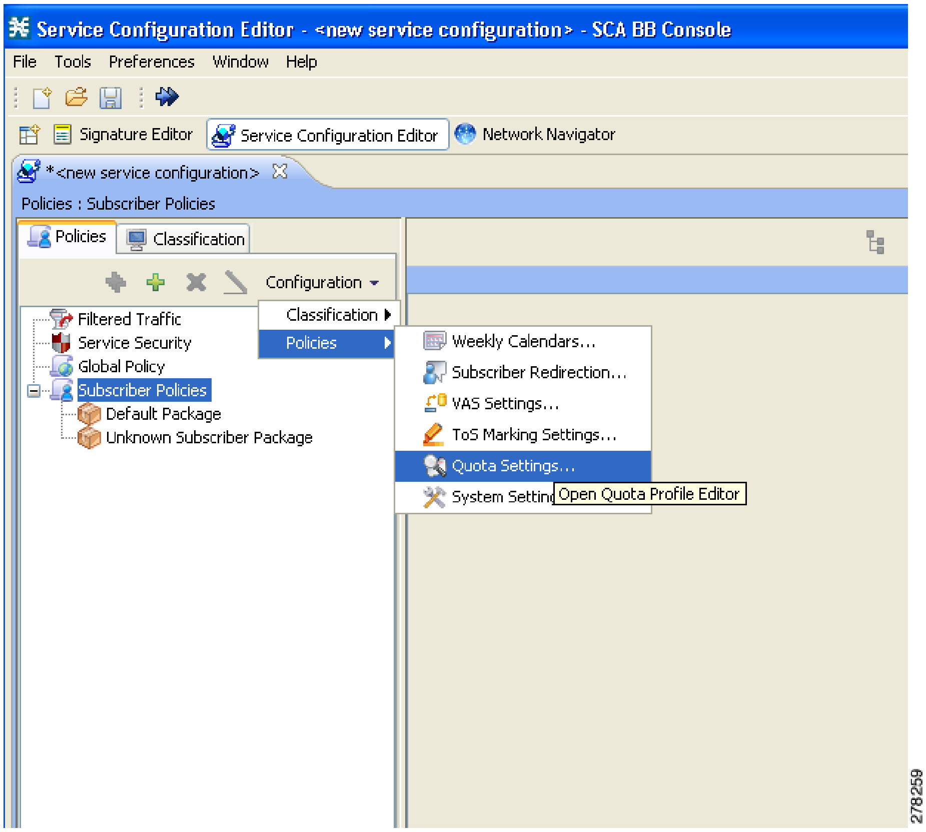
Step 4 Assign the profile to the appropriate package (Attaching the Quota Profile to a Package, page 4-17).

Step 5 Configure a rule for the package defining the action of the bucket for the relevant service in that package (Defining a Rule Using the Quota Profile, page 4-19).

Accessing the Quota Profile Editor

To access the Quota Profile Editor, choose **Service Configuration** > **Configuration** > **Policies** > **Quota Settings**

Figure 4-6 Accessing the Quota Profile Editor


Service Configuration Editor - <new service configuration> - SCA BB Console
File Tools Preferences Window Help
Signature Editor
Service Configuration Editor
Network Navigator
*<new service configuration>
Policies : Subscriber Policies
Policies
Classification
Configuration
Filtered Traffic
Service Security
Global Policy
Subscriber Policies
Default Package
Unknown Subscriber Package
Classification
Policies
Weekly Calendars...
Subscriber Redirection...
VAS Settings...
ToS Marking Settings...
Quota Settings...
System Settin
Open Quota Profile Editor
278259

Global Quota Configuration

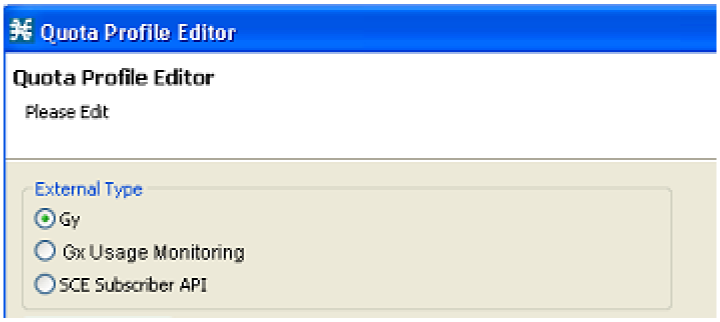
There are two aspects of global quota configuration:

- Selecting the external quota type (Gy or SCE Subscriber API)
- Configuring the Quota Manager general settings

Configuring the External Quota Type

The external quota type options are displayed in the upper part of the Quota Profile Editor, as shown in Figure 4-7. The default quota type is Gy.

Figure 4-7 Quota Profile Editor Screen



Quota Profile Editor

Quota Profile Editor

Please Edit

External Type

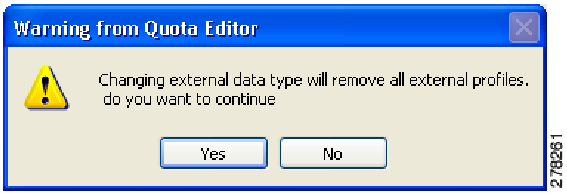
● Gy

○ Gx Usage Monitoring

○ SCE Subscriber API

Changing the external quota type may result in the loss of the existing user-defined quota profile data. Therefore, if you change the quota type after creating any quota profiles, the system issues a warning and asks for confirmation, as shown in Figure 4-8.

Figure 4-8 Warning from Quota Editor Message



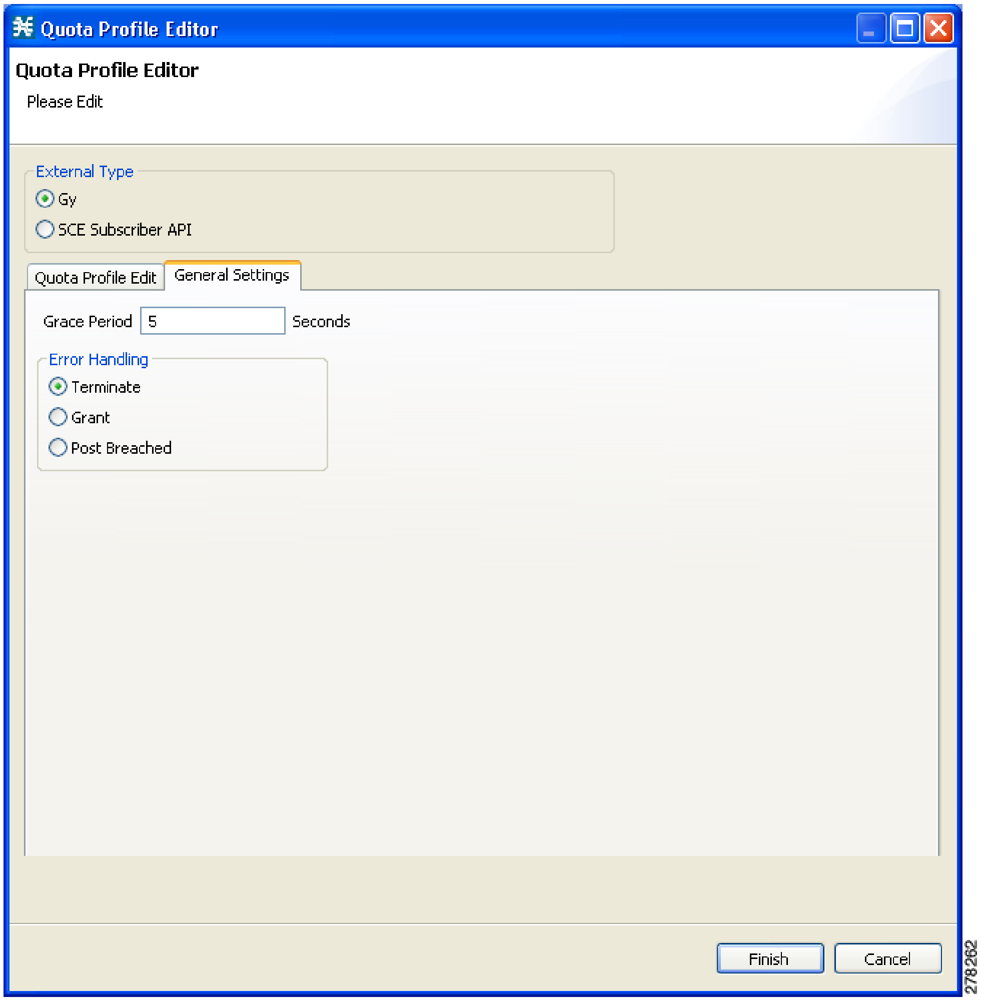
Warning from Quota Editor

Changing external data type will remove all external profiles.
do you want to continue

Configuring the Quota Manager General Settings

You can configure the general quota settings from the General Settings tab of the Quota Profile Editor, as shown in Figure 4-9.

Figure 4-9 *Quota Profile Editor - General Settings Tab*



External Type

● Gy
○ SCE Subscriber API

Grace Period 5 Seconds

Error Handling

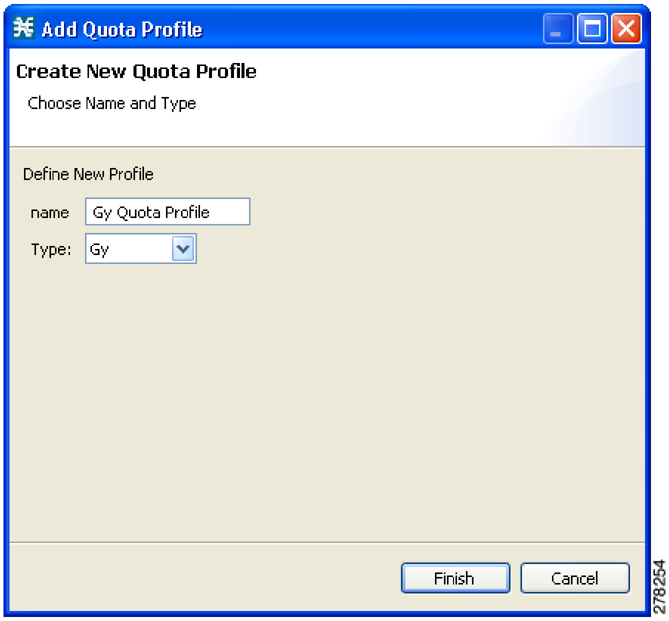
● Terminate
○ Grant
○ Post Breached

Adding a Quota Profile

Step 1 Click **New** in the Profile Edit tab.

Step 2 Enter the profile name (or you can simply accept the default name suggested by the system) and select the profile type:

Figure 4-10 Adding a Quota Profile



Add Quota Profile

Create New Quota Profile

Choose Name and Type

Define New Profile

name: Gy Quota Profile

Type: Gy

Step 3 Click **Finish**.

Editing a Quota Profile

After creating a quota profile, you can configure each bucket separately. For Gy quota profiles, you can configure the following for each bucket:

- Bucket tab:
  - Whether to request quota on login
  - Various quota time limits
  - Final action
- Service tab—Attach services to the bucket.
- Timeframe tab—Attach services per timeframe.

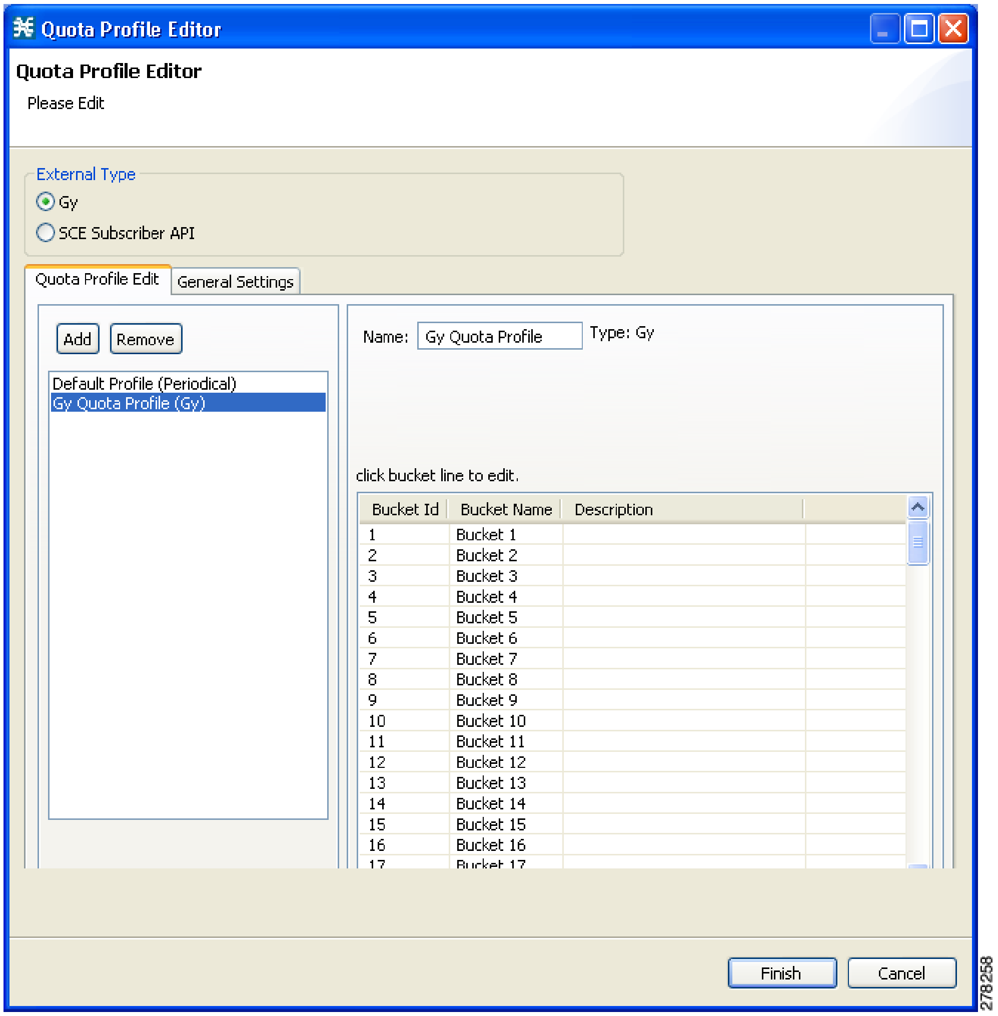
Note You cannot edit the default profile.

To configure a quota profile, complete the following steps:

Step 1 Click the profile name in the left pane.

The profile name and the individual buckets appear in the right pane.

Figure 4-11 Quota Profile Editor - Quota Profile Edit Tab



Quota Profile Editor

Quota Profile Editor

Please Edit

External Type

● Gy

○ SCE Subscriber API

Quota Profile Edit | General Settings

Add | Remove

Default Profile (Periodical)

Gy Quota Profile (Gy)

Name: Gy Quota Profile Type: Gy

click bucket line to edit.

Bucket Id	Bucket Name	Description
1	Bucket 1	
2	Bucket 2	
3	Bucket 3	
4	Bucket 4	
5	Bucket 5	
6	Bucket 6	
7	Bucket 7	
8	Bucket 8	
9	Bucket 9	
10	Bucket 10	
11	Bucket 11	
12	Bucket 12	
13	Bucket 13	
14	Bucket 14	
15	Bucket 15	
16	Bucket 16	
17	Bucket 17	

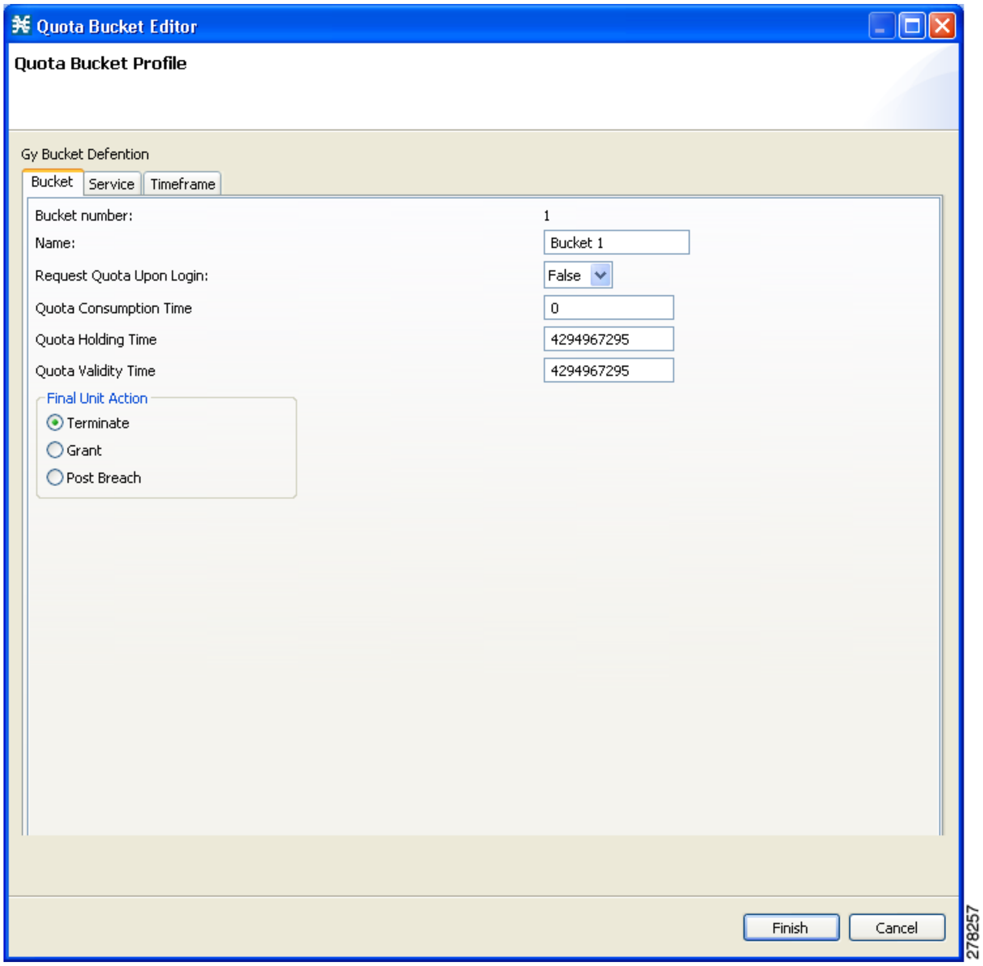
Step 2 Double-click the desired bucket to edit it.

The Quota Bucket Editor opens.

Step 3 Configure the bucket.

- General bucket configuration—Use the Bucket tab. See Figure 4-12.

Figure 4-12 Quota Bucket Editor - Bucket Tab



Quota Bucket Profile

Gy Bucket Defention

Bucket number:	1
Name:	Bucket 1
Request Quota Upon Login:	False
Quota Consumption Time	0
Quota Holding Time	4294967295
Quota Validity Time	4294967295

Final Unit Action

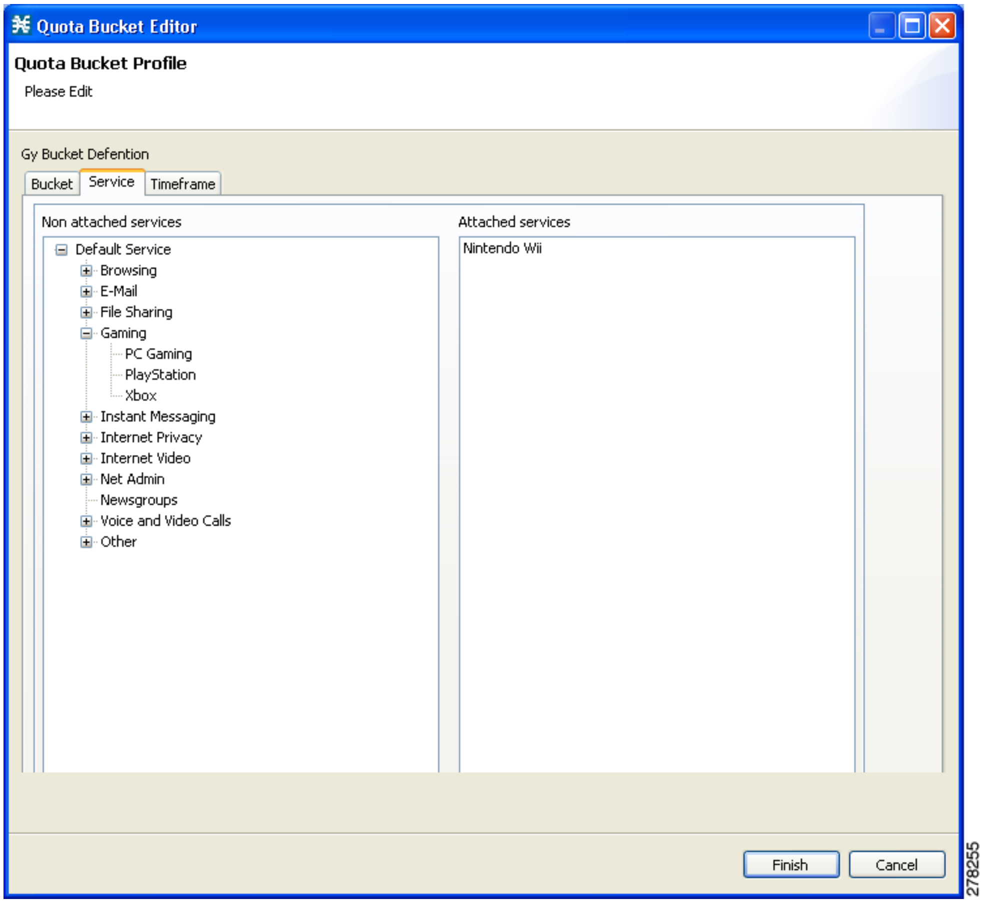
- ● Terminate
- ○ Grant
- ○ Post Breach

- Attaching services to the bucket:
  - To attach services to the bucket for all time frames, use the Service tab (see Figure 4-13). Drag the service name and drop it under **Attached services**.

    The services on the left pane are organized according to the service tree.

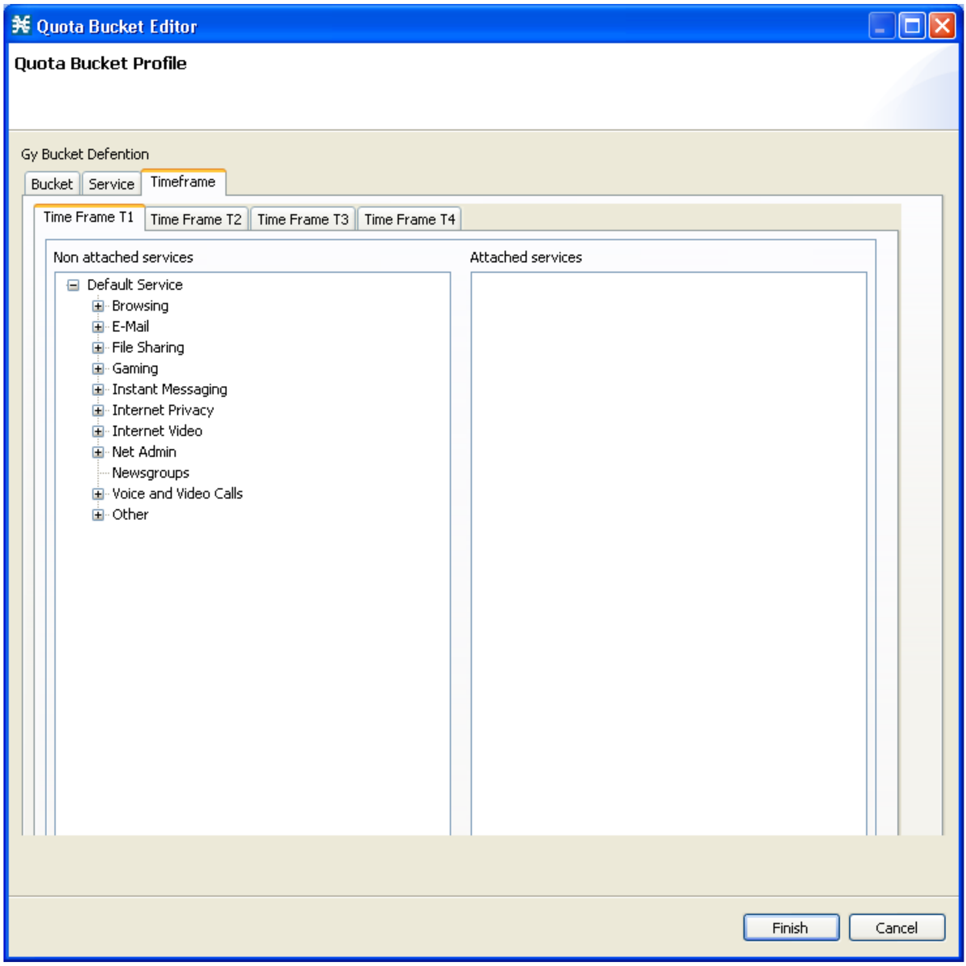
    If you drag a service, all its subservices in the tree are dragged as well.

Figure 4-13 Quota Bucket Editor - Service Tab



– To attach different services depending on the timeframe, use the Timeframe tab (see Figure 4-14). Drag the service name and drop it under **Attached service**s on the desired Time Frame tab.

Figure 4-14 Quota Bucket Editor - Timeframe Tab



Quota Bucket Editor

Quota Bucket Profile

Gy Bucket Defention

Step 4 Click **Finish**.

Step 5 Click **Finish** again.

Attaching the Quota Profile to a Package

You must attach the quota profile to the appropriate package.

To attach the quota profile to a package:

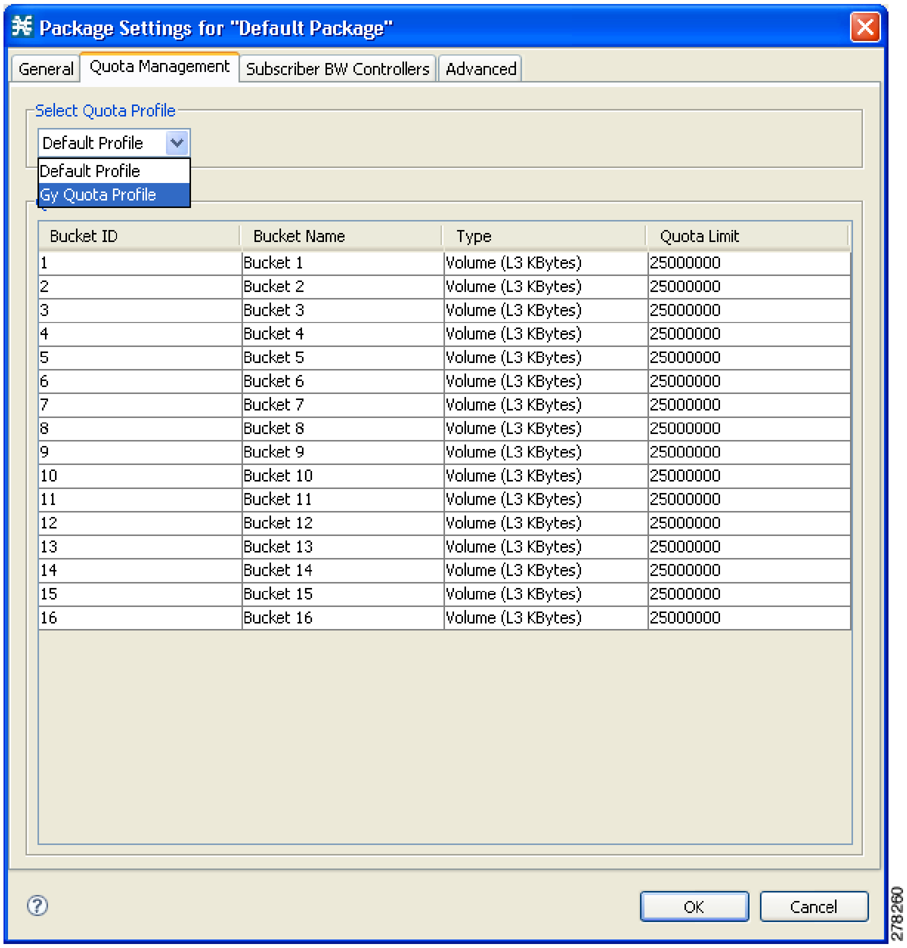
Step 1 Right-click the package in the **Policies** tab of the Service Configuration window to access the Package Settings screen.

Step 2 Click **Edit Package**.

Step 3 Click the **Quota Management** tab.

Step 4 Select the desired profile from the **Select Quota Profile** drop-down list (see Figure 4-15).

Figure 4-15 Package Settings – Quota Management Tab


Package Settings for "Default Package"
General
Quota Management
Subscriber BW Controllers
Advanced
OK
Cancel
278260

Select Quota Profile: Default Profile

- Default Profile
- Gy Quota Profile

Bucket ID	Bucket Name	Type	Quota Limit
1	Bucket 1	Volume (L3 KBytes)	25000000
2	Bucket 2	Volume (L3 KBytes)	25000000
3	Bucket 3	Volume (L3 KBytes)	25000000
4	Bucket 4	Volume (L3 KBytes)	25000000
5	Bucket 5	Volume (L3 KBytes)	25000000
6	Bucket 6	Volume (L3 KBytes)	25000000
7	Bucket 7	Volume (L3 KBytes)	25000000
8	Bucket 8	Volume (L3 KBytes)	25000000
9	Bucket 9	Volume (L3 KBytes)	25000000
10	Bucket 10	Volume (L3 KBytes)	25000000
11	Bucket 11	Volume (L3 KBytes)	25000000
12	Bucket 12	Volume (L3 KBytes)	25000000
13	Bucket 13	Volume (L3 KBytes)	25000000
14	Bucket 14	Volume (L3 KBytes)	25000000
15	Bucket 15	Volume (L3 KBytes)	25000000
16	Bucket 16	Volume (L3 KBytes)	25000000

Step 5 Click **OK.**

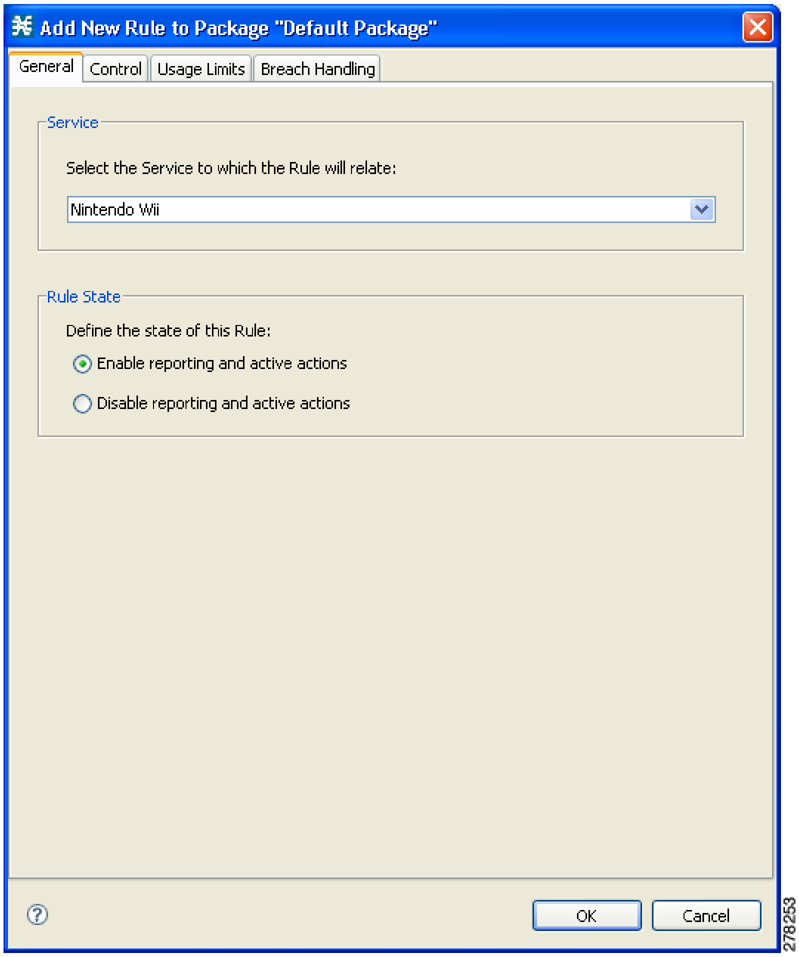
Defining a Rule Using the Quota Profile

You must add a rule to the package that defines the action when the bucket exceeds its quota.

Step 1 Click the Add icon in the right pane in the **Policies** tab of the Service Configuration window to add a rule.

Step 2 In the **General** tab, select the service attached to the bucket in the quota profile (see Figure 4-16).

Figure 4-16 Add New Rule – General Tab



Add New Rule to Package "Default Package"

Service

Select the Service to which the Rule will relate: Nintendo Wii

Rule State

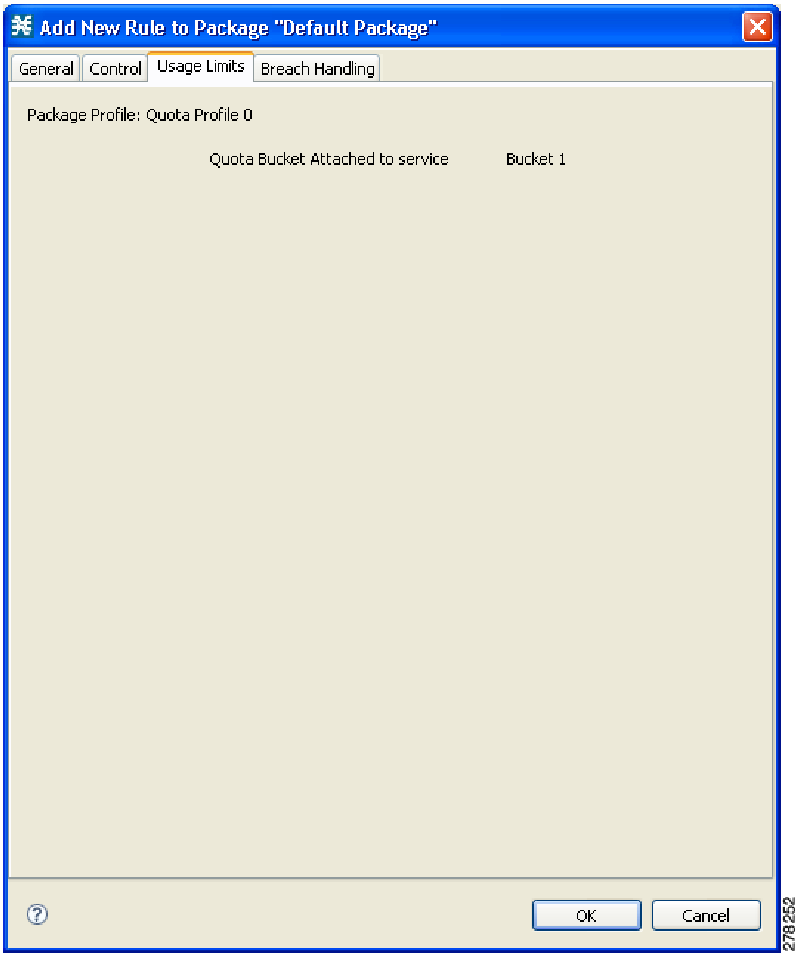
Define the state of this Rule:

● Enable reporting and active actions

○ Disable reporting and active actions

The bucket associated with this service in the quota profile is displayed in the Usage Limits tab as shown in Figure 4-17.

Figure 4-17 Add New Rule – Usage Limits Tab



Package Profile: Quota Profile 0

Quota Bucket Attached to service Bucket 1

Step 3 Configure the **Control** and **Breach Handling** parameters.

Note For more information on configuring rules, see the Cisco Service Control Application for Broadband User Guide.

Charging ID Mapping Table

The charging ID mapping table allows you to map the SCA BB parameters of package and bucket to the Gy interface parameters of service and rating group. This mapping ensures that a specified bucket from a specified package would always be output by the Gy interface as a particular service and rating group.

Charging ID Mapping Table Guidelines

- The translation is done only if the mapping table is not empty.
  - If the mapping table is not empty, and there is a corresponding entry in the table, the translation is done to the configured numbers.
  - If the mapping table is not empty, but there is no corresponding entry in the table, an appropriate error counter is increased.
- In case of "hybrid" configurations, when the translation is required for only a specified set of entries, you must configure "loop-back" entries that map the entries to themselves. In other words, even though only a partial mapping is required, all the entries must be mapped in the table, including those that do not require translation. For example, package-id 5/bucket-id 7 to service-id 5/rating-group 7.
- The same service ID and rating group combination can be assigned to multiple packages within a bucket.
- The table can hold up to 2000 mappings.

Charging ID Mapping Table CLI Commands

Table 4-3 lists the CLI commands used to configure and monitor the charging ID mapping table.

Table 4-3 Charging ID Mapping Table CLI Commands

CLI Commands	Description
diameter Gy charging-id-mapping package-id <*package-id*> bucket-id <*bucket-id*> service-id <*service-id*> rating-group <*rating-group*>	Add a mapping entry. Maps the specified service-id and rating-group to the specified package-id and bucket-id.
no diameter Gy charging-id-mapping package-id <*package-id*> bucket-id <*bucket-id*>	Delete the mapping table entry for the specified package-id and bucket-id.
no diameter Gy charging-id-mapping all	Clear the charging ID mapping table.
show diameter Gy charging-id-mapping package-id <*package-id*> bucket-id <*bucket-id*>	Show the mapping table entry for the specified package-id and bucket-id.
show diameter Gy charging-id-mapping	Show the complete charging ID mapping table.

Example for mapping the first three buckets in package-id 5 to service-id 1 and rating-groups 10-12:

```
diameter Gy charging-id-mapping package-id 5 bucket-id 1 service-id 1 rating-group 10
diameter Gy charging-id-mapping package-id 5 bucket-id 2 service-id 1 rating-group 11
diameter Gy charging-id-mapping package-id 5 bucket-id 3 service-id 1 rating-group 12
```

Gy Interface Failover Support

The Gy interface failure support in fault situations is governed by the value of two AVPs:

- Credit-Control-Failure-Handling (CCFH)
- Credit-Control-Session-Failover (CCSF)

The default values of these two attributes can be configured locally in the SCE. The default CCFH value is TERMINATE and the default CCSF value is “Failover not Supported”. The OCS can override the default values by sending the two AVPs in a CCA message.

When the Gy interface receives a Result-Code 4xxx, it retransmits the message to the original server.

If the CCSF and CCFH AVPs are carried by a CCA message, the AVP values are applied only to the session they are communicated on.

The Gy interface implements its failover decision based on whether a failover is needed or not. The Gy interface uses the peer table and failover mode to decide which destination each message should be sent to. For each Gy CCR message, the Gy interface checks the peer table and failover mode for the correct destination information.

For additional details of the Gy interface failover support, see the “Diameter Load Balancing and High Availability Schemes” section on page 2-5, the “High Availability for the Gx Interface” section on page 3-10, and the following sections:

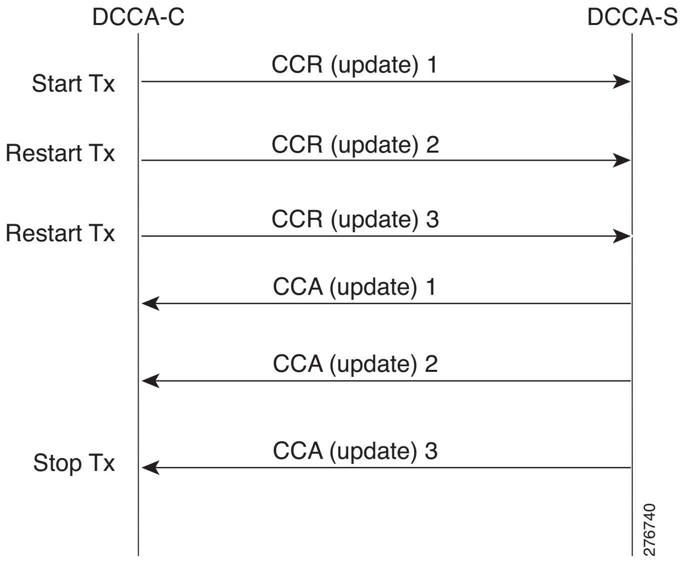
- Tx Timer, page 4-22
- CCSF, page 4-23
- CCFH, page 4-24
- Gy Failover Decisions, page 4-24
- Failure Handling of an Initial CCR Message, page 4-25
- Failure Handling of an Updated CCR Message, page 4-25
- DCCA Event Tables, page 4-25
- Detailed Flow Charts for Failover Scenarios, page 4-30
- Cascade Failover, page 4-31

Tx Timer

Usually the diameter layer detects any transport failure within the diameter server; but for prepaid services, the subscriber expects an answer from the network in a reasonable time. Therefore, a Tx timer is used by the DCCA client to supervise the communication with the server. When the Tx time expires, the DCCA client takes action based on the current value of CCFH for the CC-session-id.

The Tx timer is restarted for each initial CCR message and for each updated CCR message. Because multiple concurrent update CCR messages are possible, if one update CCR message is pending, a subsequent update CCR message restarts the Tx timer. When answers to all pending update CCR messages are received, the Tx timer is stopped. Figure 4-18 illustrates the Tx timer behavior.

Figure 4-18 Tx Timer Behavior



CCSF

The forwarder makes forwarding decisions based on CCSF value as passed to it from the Gy interface. If the value is FAILOVER_NOT_SUPPORTED, a CC session is never moved to an alternate server. If the value is FAILOVER_SUPPORTED, the forwarder attempts to move the session to an alternate server if the Gy interface asks for an alternate server.

The following events trigger the forwarder to make a forwarding decision:

- Receipt of a protocol error with the following Result-Code AVP values.
  - DIAMETER_UNABLE_TO_DELIVER
  - DIAMETER_TOO_BUSY
  - DIAMETER_LOOP_DETECTED
- Expiration of the Tx timer without receipt of Watch Dog Answer (WDA) message.
- Transmission failure of the CCR message.

CCFH

Table 4-4 lists the actions on the session for each value of CCFH.

Table 4-4 CCFH Value and Action on Session

CCFH Value	Action on Session
CONTINUE	Allows the session and user traffic to continue. If an alternate server exists and failover is supported, the Forwarder should direct the traffic to the alternate server. Otherwise the Gy client sends an error to the SCA BB with the subscriber name and SCA BB grants a predefined quota for the subscriber.
TERMINATE	Terminates the session and the CC session.
RETRY_AND_TERMINATE	Allows the session and user traffic to continue. The DCCA client retries an alternate server and if failure to send condition occurs, the session is terminated.

CCFH Values and the Corresponding Actions on the Session

The following are the fault conditions in which CCFH is used to determine the action on the session:

- Expiration of the Tx timer.
- Receipt of a CCA message with a protocol error.
- Receipt of a failed CCA; for example, receipt of a CCA with a permanent failure notification.
- Failed send condition action. (The DCCA client is not able to communicate with the desired destination or is unable to communicate with a defined alternative destination when failover is supported.)

The CCFH value is used both for session-level errors and bucket-level errors.

Bucket-level errors such as DIAMETER_CREDIT_LIMIT_REACHED do not cause failover.

Gy Failover Decisions

The Gy interface communicates to the forwarder when a failover is required for a server per session. The client then expects to receive an alternate server. The alternate server may be the currently assigned server, depending on the configured forwarder scheme.

The Gy interface communicates to the forwarder and requests an alternate server in the following situations:

- Severe Failure Situation: CCSF is FAILOVER_IS_SUPPORTED and one of the following takes place:
  - The following Result-Code AVP values appear in the CCA:

    DIAMETER_UNABLE_TO_DELIVER

    DIAMETER_TOO_BUSY

    DIAMETER_LOOP_DETECTED
  - Diameter Stack Error

- Failure Situation—CCSF is FAILOVER_IS_SUPPORTED and CCFH is CONTINUE or RETRY_TERMINATE, failure is not bucket level, and one of the following situations occurs:
  - Expiration of the Tx timer
  - Receipt of a CCA with protocol error
  - Receipt of a failed CCA; for example, CCA with a permanent failure notification

Failure Handling of an Initial CCR Message

When the initial CCR message is sent on a CC-session, the Tx timer is started and the CC-session is pending awaiting a CCA message. When the Tx timer expires before the initial CCA message is received, the action on the session context is determined by the CCFH.

- If the CCFH value is CONTINUE, the session is moved to the alternate server by the forwarder and a CCR INITIAL message is not sent (configurable). If the message to the alternate fails, the session context is terminated and a “Grant Session” message is sent to the SCA BB.
- If the CCFH value is RETRY_AND_TERMINATE, the Gy interface tries an alternate server. If it fails, the session context is terminated and a “Terminate Session” message is sent to the SCA BB. The SCA BB notifies the subscriber that the session is terminated.
- If the CCFH value is TERMINATE, the session context is terminated and a “Terminate Session” is sent to the SCA BB. The SCA BB notifies the subscriber that the session is terminated.

Failure Handling of an Updated CCR Message

When an update CCR message is sent on a CC_session, the Tx timer is started and the CC-session state is pending awaiting a CCA message. When the Tx timer expires before the initial CCA message is received, the action on the session context is determined by the CCFH.

- If CCFH value is CONTINUE, the session is moved to the alternate server by the Forwarder and the traffic continues with an update CCR message. If the alternate fails, a “Grant Service” message is sent to the SCA BB.
- If CCFH value is RETRY_AND_TERMINATE, the Gy client tries to retransmit. If the retransmit fails, the Gy interface sends a “Terminate Service” message to the SCA BB. If an update CCA message arrives later, it is ignored.

DCCA Event Tables

The Gy interface supports session-based credit control when the first interrogation is executed after the authorization or authentication process.

In Table 4-5 and Table 4-6, the “failure to send” event means that the Gy interface is unable to communicate with the desired destination or, if failover procedure is supported, with a defined alternative destination (for example, the request timed out and the answer message is not received). This can be due to the peer being down or due to a physical link failure in the path to or from the OCS.

The 'Temporary error' event means that the Gy interface received a protocol error notification (DIAMETER_TOO_BUSY, DIAMETER_UNABLE_TO_DELIVER, or DIAMETER_LOOP_DETECTED) in the Result-Code AVP of the Credit-Control-Answer command. The protocol error notification can be received in answer to the retransmitted request to a defined alternative destination, if failover is supported.

The 'Failed answer' event means that the Gy interface received a nontransient failure (permanent failure) notification in the CCA command. The permanent failure notification may ultimately be received in answer to the retransmitted request to a defined alternative destination, if failover is supported.

The Tx timer, which is used to control the waiting time in the Gy interface in the Pending state, is stopped upon exit of the Pending state. The stopping of the Tx timer is omitted in the state machine when the new state is Idle, because moving to Idle state indicates the clearing of the session and all the variables associated to it.

In Table 4-5 and Table 4-6, the failover to a secondary server upon “Temporary error” or “Failure to send” is not described. Moving an ongoing credit-control message stream to an alternate server is, however, possible if the CC-Session-Failover AVP is set to FAILOVER_SUPPORTED.

Table 4-5 Client Session-Based First Interrogation Events Versus Actions

	Action	
Event	**SCA BB**	**Gy Client**
Client or device requests access/service	Send Session Creation RDR.	—
	—	Gy interface sends CC initial request, starts Tx (OpenBlox).
Successful CC initial answer received	—	Gy interface stop Tx (OpenBlox).
Failure to send, or temporary error and CCFH equal to CONTINUE	—	Notify SCA BB “Grant Session” to end user.
Failure to send, or temporary error and CCFH equal to TERMINATE or to RETRY_AND_TERMINATE	—	Notify “Terminate Session” to SCA BB.
Tx expired and CCFH equal to TERMINATE	—	Notify SCA BB “Terminate Session” to end user.
Tx expired and CCFH equal to CONTINUE or to RETRY_AND_TERMINATE	—	Notify SCA BB “Grant Session” to end user.
CC initial answer received with result code END_USER_SERVICE_DENIED or USER_UNKNOWN	—	Notify “Terminate Session” to SCA BB.
CC initial answer received with result code equal to CREDIT_CONTROL_NOT_APPLICABLE	—	Notify SCA BB “Grant Session” to end user.
Failed CC initial answer received and CCFH equal to CONTINUE	—	Notify SCA BB “Grant Session” to end user.
Failed CC initial answer received and CCFH equal to TERMINATE or to RETRY_AND_TERMINATE	—	Notify “Terminate Session” to SCA BB

Table 4-5 Client Session-Based First Interrogation Events Versus Actions (continued)

	Action	
Event	SCA BB	Gy Client
User service terminated	SCA BB sends Status Update.	—
	—	Send CCR UPDATE
User Logout	SCA BB sends Session Termination.	—
	—	Send CCR TERMINATE.
Change in rating condition	—	Special treatment.

Table 4-6 Client Session-Based Intermediate and Final Interrogations Events Versus Actions

	Action	
Event	SCA BB	Gy Client
Granted unit elapses and no final unit indication received	SCA BB Sends Quota Status RDR.	—
	—	Gy interface sends CC update request, start Tx.
Granted unit elapses and final unit action equal to TERMINATE received	—	SCA BB is notified with Final Unit Indication.
	SCA BB sends Quota Status Update with (reporting reason final).	—
	—	When RDR is received, CC UPDATE per this bucket-id request is sent wit FINAL reporting reason.
Change in rating condition in queue	—	Special treatment.
User Service terminated	SCA BB sends Status Update RDR (reporting reason final).	—
	—	Gy interface sends CC UPDATE per this bucket-id with Final Reporting Reason. Start Tx.
User Logout	SCA BB sends Status Termination RDR	—
	—	Gy interface sends CC Terminate.

Table 4-6 Client Session-Based Intermediate and Final Interrogations Events Versus Actions

Event	Action	
	SCA BB	**Gy Client**
Validity-Time elapses	SCA BB sends Status Update RDR	—
	—	Gy interface sends CC update request. Start Tx.
RAR received	—	Gy client sends RAA. Gy notifies SCA BB to send status update.
	SCA BB to send Status Update	—
	—	Gy interface sends CC update request. Start Tx.
Successful CC update answer received	—	Stop Tx.
Failure to send, or temporary error and CCFH equal to CONTINUE	—	Notify SCA BB “Grant Service” to end user.
Failure to send, or temporary error and CCFH equal to TERMINATE or to RETRY_AND_TERMINATE	—	Notify “Terminate Service” to SCA BB.
Tx expired and CCFH equal to TERMINATE	—	Notify “Terminate Service” to SCA BB.
Tx expired and CCFH equal to CONTINUE or to RETRY_AND_TERMINATE	—	Notify SCA BB “Grant Service” to end user.
CC update answer received with result code END_USER_SERVICE_DENIED	—	Notify “Terminate Service” to SCA BB.
CC update answer received with result code equal to CREDIT_CONTROL_NOT_APPLICABLE	—	Notify SCA BB “Grant Service” to end user.
Failed CC update answer received and CCFH equal to CONTINUE	—	Notify SCA BB “Grant Service” to end user.

Table 4-6 Client Session-Based Intermediate and Final Interrogations Events Versus Actions

	Action	
Event	**SCA BB**	**Gy Client**
Failed CC update answer received and CCFH equal to TERMINATE or to RETRY_AND_TERMINATE	—	Notify “Terminate Service” to SCA BB.
Successful CC termination answer received	—	—

Detailed Flow Charts for Failover Scenarios

Figure 4-19 depicts the Gy client behavior upon CCA error or timeout error scenarios.

Figure 4-19 Gy Client Behavior Upon CCA Error or Timeout Error

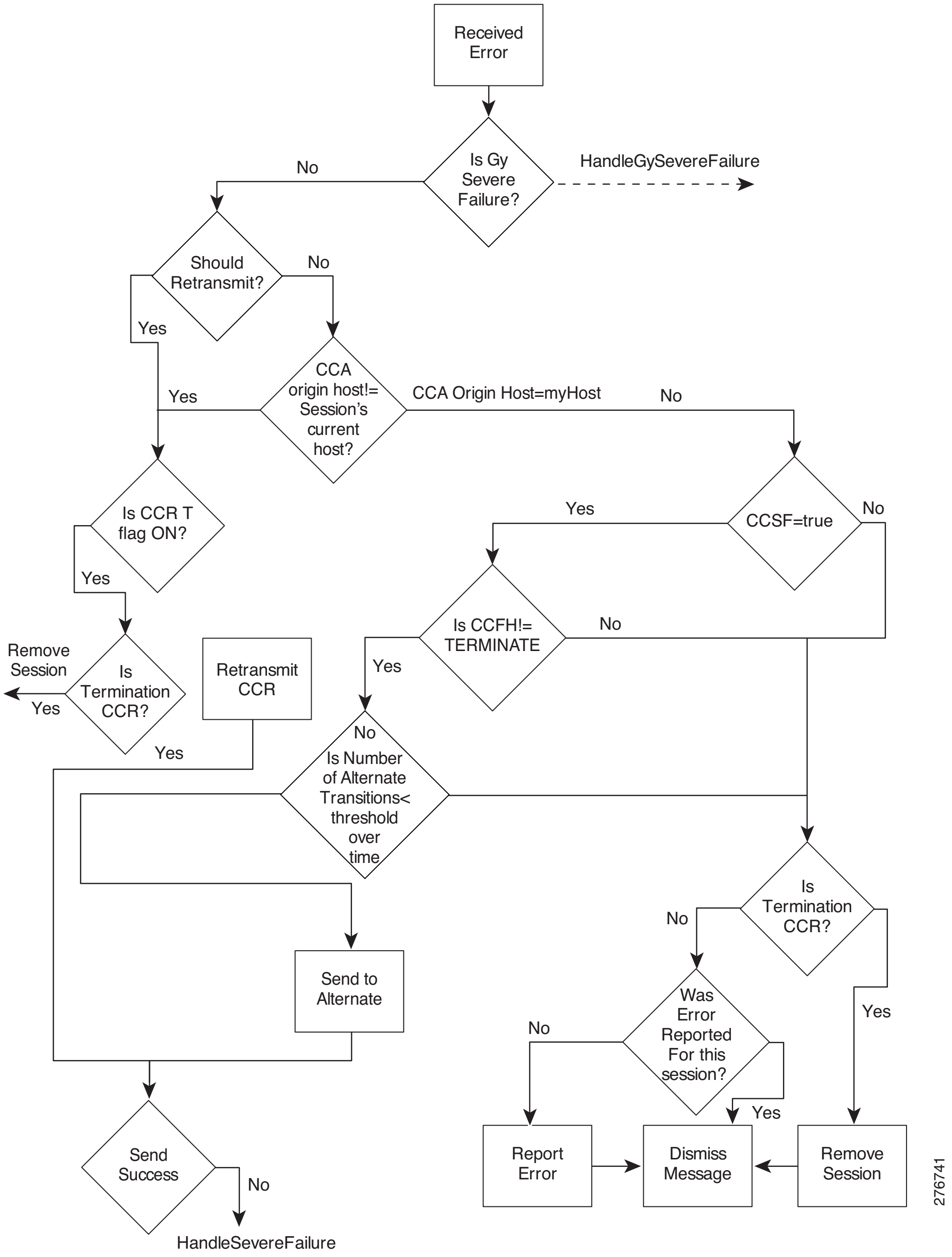
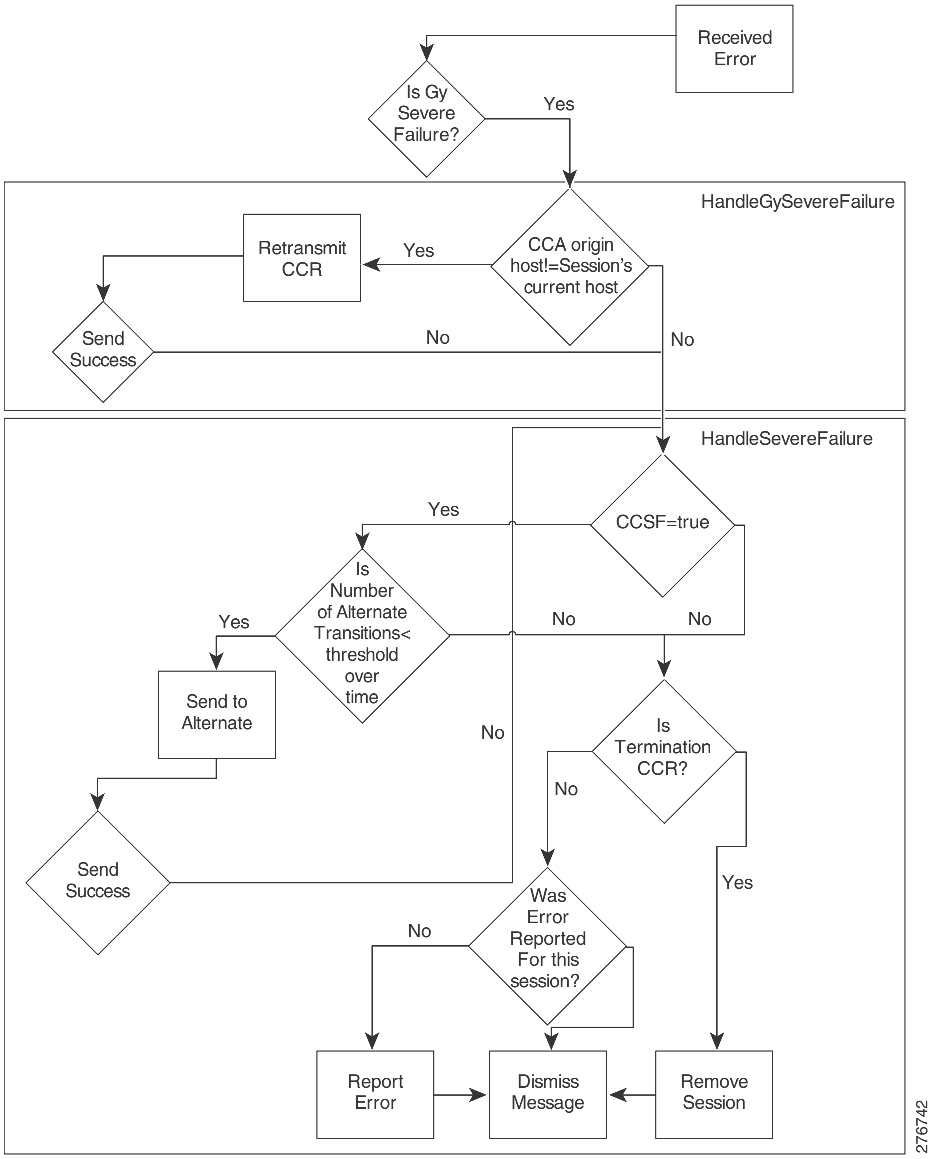


Figure 4-20 depicts the Gy client behavior upon severe failure situation.

Figure 4-20 Gy Client Behavior Upon Severe Failure



Cascade Failover

Upon cascade failover, the secondary box has no sessions in the session database.

Each quota status update that does not have a session on the secondary box creates a new session context and is sent an updated CCR.

Sessions that are left open on the OCS are closed by aging or by identifying a new session with the same subscription ID.

CHAPTER 5

Gx RLS9 Interface Support

Revised: March 29, 2012, OL-24167-04

Introduction

The Gx RLS9 interface uses only the Gx interface (no Gy interface) to provide support to the following scenarios:

- Fair usage at bearer level; requires reporting usage volume per subscriber session
- Fair usage at flow level; requires reporting usage volume per subscriber flow

Support for Gx RLS9 provides Gx enhancements that extend the Gx interface to support the new usage monitoring events. The Gx RLS9 interface supports a number of new events and AVPs. The new events are in 3GPP TS 29.212 V9.1.0 (Dec. 2009).

Note Although the Gx RLS9 enhancements are in conformance with 3GPP TS 29.212, the SCE platform is not fully compliant with the 3GPP TS 29.212 standard.

Usage Monitoring and Reporting

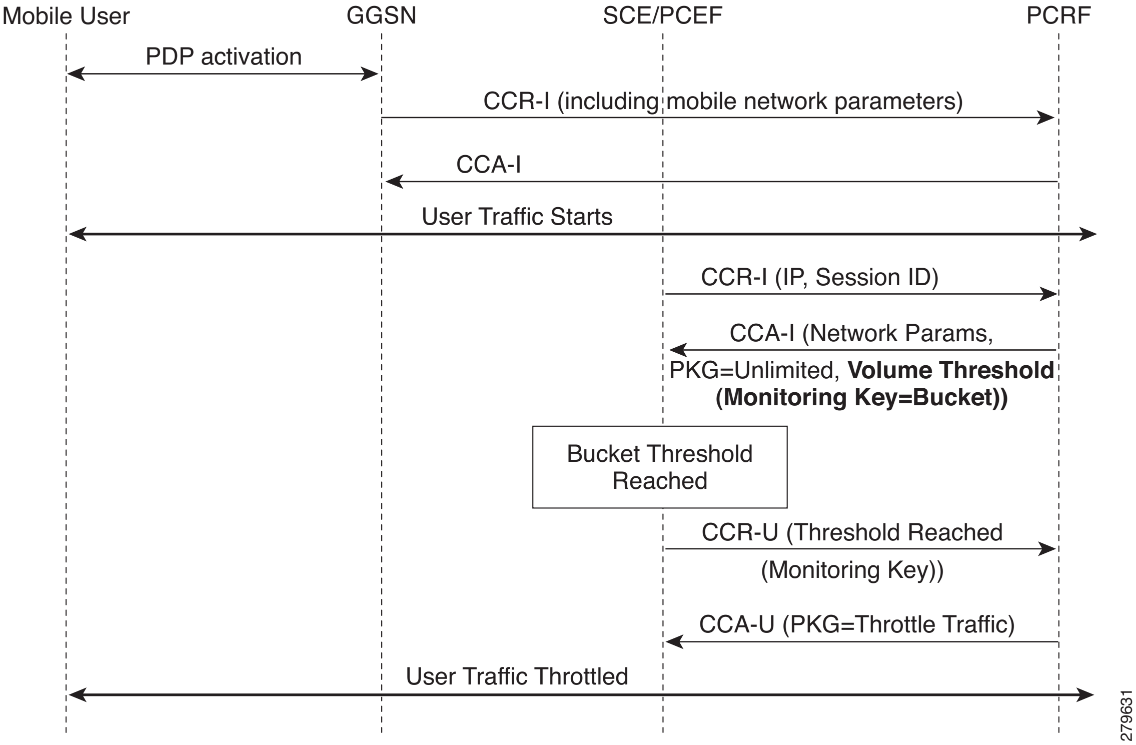
Figure 5-1 shows an example of usage monitoring—fair usage at bearer or flow level.

Usage monitoring events require a monitoring key to refer to the instance accounted. The monitoring key is set by the PCRF by using the Monitoring-Key AVP as part of the Usage-Monitoring-Information AVP. The SCE bucket ID is used as the monitoring key and is specified per package.

You can map an SCE bucket to:

- A single service
- A set of services
- All the traffic of a specific subscriber

Figure 5-1 Usage Monitoring and Reporting



In this example, the events are as follows:

1. The SCE monitors user traffic reports to the PCRF.
2. The PCRF selects the traffic to be monitored by using the monitoring-key and a threshold.
3. The PCRF sends a reporting event to be notified when the threshold is crossed.

Configuring Usage Monitoring in the SCA BB Console

In the SCA BB GUI, you can create quota profiles that define the limits and action of each monitoring key (bucket) and assign specific services to that monitoring key. You must then attach the quota profile to a package and define a quota rule for the package for the relevant service.

Note For more information on configuring and managing quotas, see the Cisco Service Control Application for Broadband User Guide.

To configure a Gx usage monitoring quota profile, complete the following steps. The steps are described in detail in the referenced sections.

Step 1 Select Gx Usage Monitoring as the External Quota Type (Configuring the External Quota Type, page 5-5).

Step 2 Create the Gx Usage Monitoring Quota Profile (Adding a Quota Profile, page 5-6).

Step 3 Assign services to the profile (Editing a Gx Usage Monitoring Quota Profile, page 5-7).

Step 4 Assign the profile to the appropriate package (Attaching the Quota Profile to a Package, page 4-17).

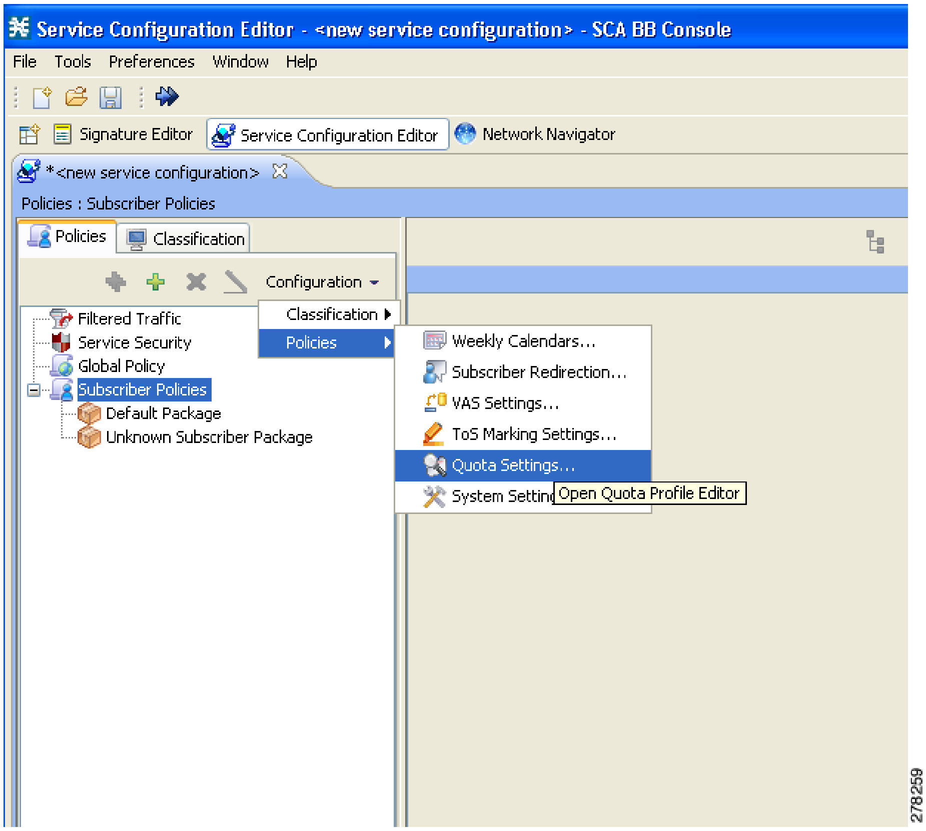
Step 5 Configure a rule for the package defining the action of the bucket for the relevant service in that package (Defining a Rule Using the Quota Profile, page 4-19).

Accessing the Quota Profile Editor

You can access the Quota Profile Editor from the Configuration menu:

Choose **Service Configuration** > **Configuration** > **Policies** > **Quota Settings.**

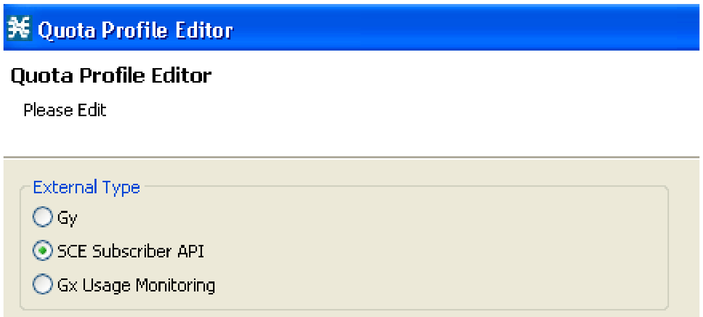
Figure 5-2 Accessing the Quota Profile Editor



Configuring the External Quota Type

The external quota type options are displayed in the upper part of the Quota Profile Editor, as shown in Figure 5-3. The default quota type is Gy.

Figure 5-3 Quota Profile Editor Screen



Quota Profile Editor

Quota Profile Editor

Please Edit

External Type

○ Gy

● SCE Subscriber API

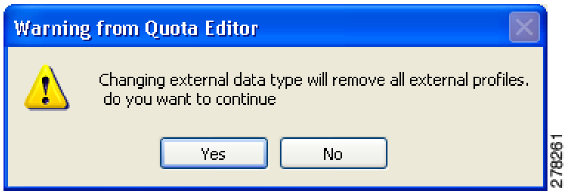
○ Gx Usage Monitoring

When Gx Usage Monitoring is selected, you cannot configure the settings in the General Settings tab, because they are set to the following preconfigured values:

- Grace Period = 2 sec
- Error Handling = Grant

Changing the external quota type may result in the loss of the existing user-defined quota profile data. Therefore, if you change the quota type after creating any quota profiles, the system issues a warning and asks for confirmation, as shown in Figure 5-4.

Figure 5-4 Warning from Quota Editor Message



Warning from Quota Editor

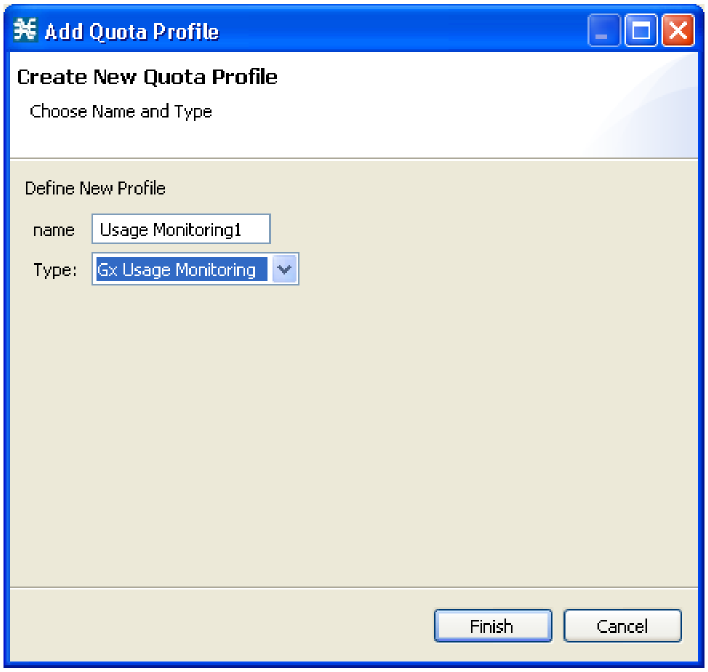
Changing external data type will remove all external profiles.
do you want to continue

Adding a Quota Profile

Step 1 In the Profile Edit tab, click **New**.

Step 2 Type in the profile name (or you can simply accept the default name suggested by the system) and select the profile type:

Figure 5-5 Adding a Quota Profile



Create New Quota Profile

Choose Name and Type

Define New Profile

name: Usage Monitoring1

Type: Gx Usage Monitoring

Step 3 Click **Finish**.

Editing a Gx Usage Monitoring Quota Profile

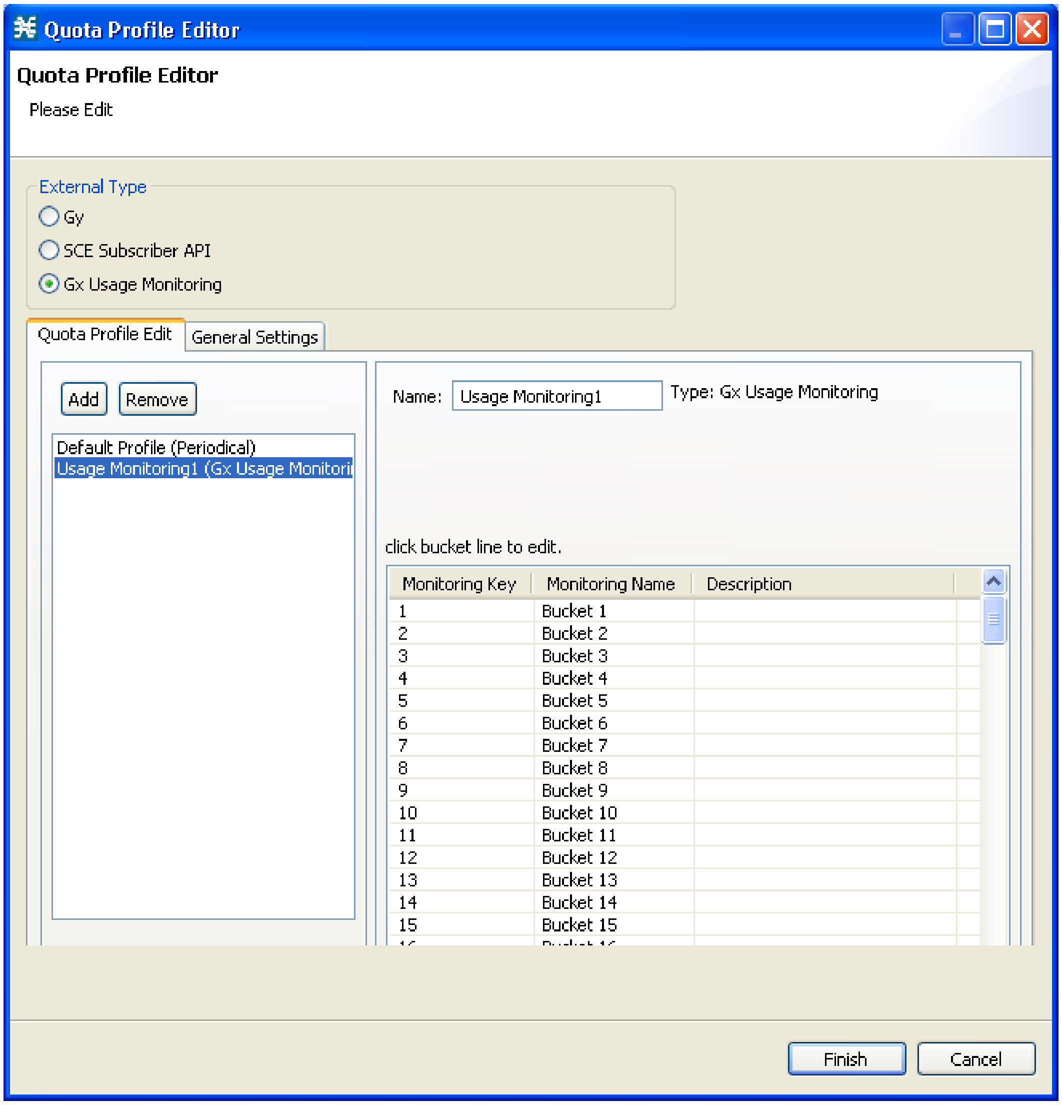
After creating a quota profile, you can configure each monitoring key separately. For Gx Usage Monitoring quota profiles, you can map services to each monitoring key.

To configure a Gx Usage Monitoring quota profile, complete the following steps:

Step 1 Click on the profile name in the left pane of the Quota Profile Editor.

The profile name and the individual monitoring keys appear in the right pane. 127 monitoring keys are supported.

Figure 5-6 Quota Profile Editor - Quota Profile Edit Tab



Quota Profile Editor

Quota Profile Editor

Please Edit

External Type

○ Gy

○ SCE Subscriber API

● Gx Usage Monitoring

Default Profile (Periodical)

Usage Monitoring1 (Gx Usage Monitori

Name: Usage Monitoring1 Type: Gx Usage Monitoring

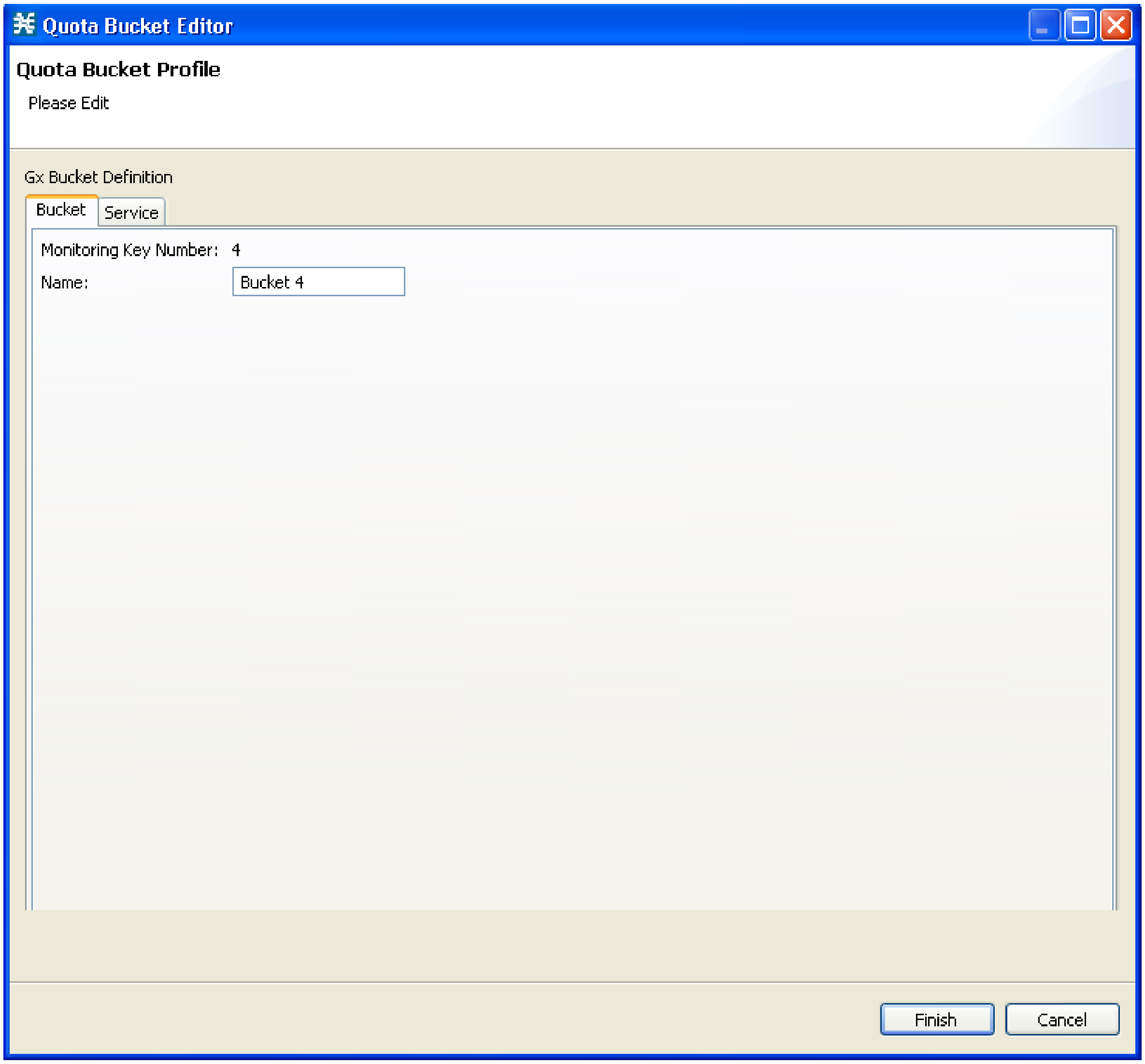
click bucket line to edit.

Monitoring Key	Monitoring Name	Description
1	Bucket 1	
2	Bucket 2	
3	Bucket 3	
4	Bucket 4	
5	Bucket 5	
6	Bucket 6	
7	Bucket 7	
8	Bucket 8	
9	Bucket 9	
10	Bucket 10	
11	Bucket 11	
12	Bucket 12	
13	Bucket 13	
14	Bucket 14	
15	Bucket 15	

Step 2 Double-click the desired monitoring key to assign services.

The Quota Bucket Editor opens. The Bucket tab simply displays the monitoring key number and the bucket number.

Figure 5-7 Quota Bucket Editor - Bucket Tab



Quota Bucket Editor

Quota Bucket Profile

Please Edit

Gx Bucket Definition

Monitoring Key Number: 4

Name: Bucket 4

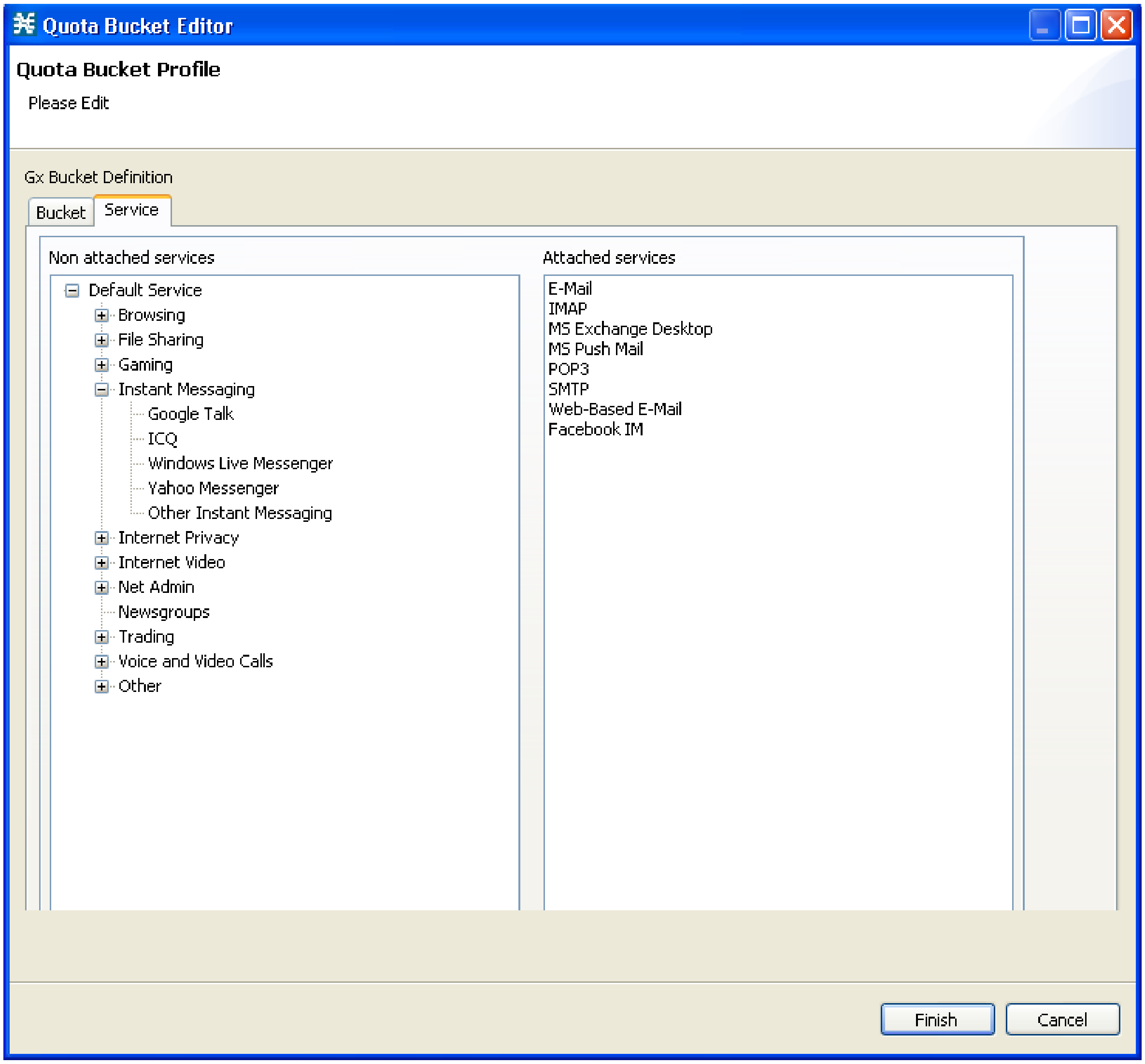
Step 3 Click the Service tab.

Step 4 Drag the service name from the left pane and drop it under **Attached services**.

The services on the left pane are organized according to the service tree.

If you drag a service then all its sub-services in the tree are dragged as well.

Figure 5-8 Quota Bucket Editor-Service Tab



Quota Bucket Profile

Please Edit

Gx Bucket Definition

Non attached services

- Default Service
  - Browsing
  - File Sharing
  - Gaming
  - Instant Messaging
    - Google Talk
    - ICQ
    - Windows Live Messenger
    - Yahoo Messenger
    - Other Instant Messaging
  - Internet Privacy
  - Internet Video
  - Net Admin
  - Newsgroups
  - Trading
  - Voice and Video Calls
  - Other

Attached services

E-Mail
IMAP
MS Exchange Desktop
MS Push Mail
POP3
SMTP
Web-Based E-Mail
Facebook IM

Step 5 Click **Finish**.

Step 6 Click **Finish** again.

CHAPTER 6

Capturing and Reporting Subscriber Attributes

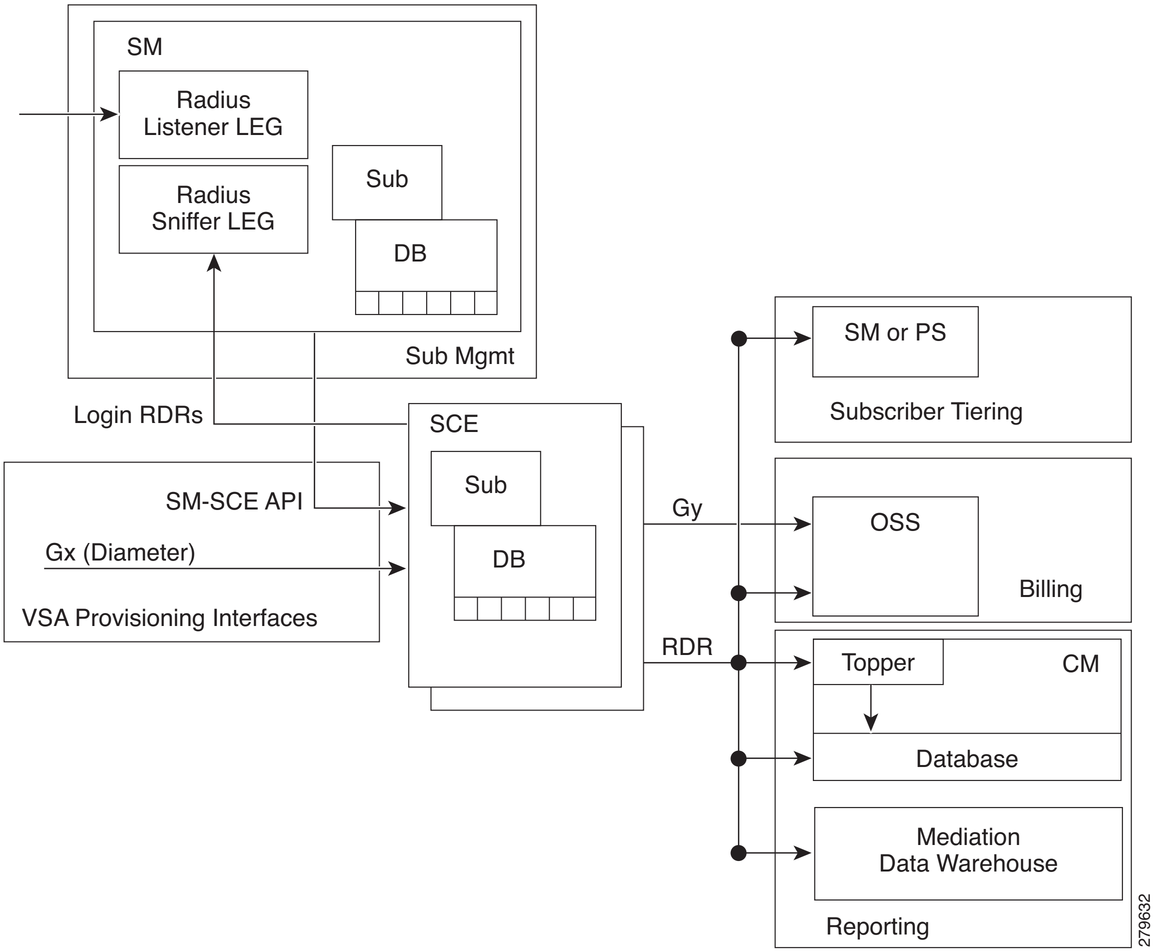
Revised: March 29, 2012, OL-24167-04

Introduction

Vendor Specific Attributes (VSA) are RADIUS or Diameter attributes that are sent mostly in mobile environments. They can be captured from the traffic processed by the SCE and then reported to the billing server. They can also be sent to the Collection Manager in various RDRs to be used to generate a number of common mobile reports.

Figure 6-1 shows a high-level diagram of the Cisco Service Control mobile solution including capturing and reporting subscriber attributes.

Figure 6-1 System Block Diagram



Capturing Subscriber Attributes

VSAs can be captured by using either of the following entities:

- The Cisco SCE platform
- The RADIUS Login Event Generator (LEG)

Only the VSAs that you select are captured. You can choose which attributes are relevant, and store and process only those attributes. You can select a maximum of 20 attributes from the list of available VSAs. The list of attributes to capture can be modified while the system is running.

The following data structures are used to capture and store VSAs:

- Dictionary table—A table that contains all the supported attributes, with the following information for each attribute:
  - Attribute name
  - Protocol (RADIUS/Diameter/GTP-C)
  - Input type
  - Type used in the database (usually the same as input type)
  - Attribute ID
  - VSA (yes/no)
  - Vendor ID (if used by VSA)

  The local attribute table reads the attribute details from this table.
- Local attribute table—A global table (for all the subscribers and all the packages) that holds all the details for the selected attributes and parameters.

  The Gx interface, Gy interface, and the subscriber database use this table to obtain information for each configured attribute.
- Subscriber attribute database— A table of captured attributes per subscriber. A subscriber attribute database is maintained in both the SCE and the SM. Information captured by either entity is provisioned from that entity to the other entity so that the subscriber attribute database is always current in both the SCE and the SM.

Constraints and Limitations

- Only one session per subscriber is supported. A subscriber with multiple Access Point Names (APN) or multiple devices used at the same time can be separated into separate subscribers by adding the APN or device into the subscriber ID.
- Scale limitations—When supporting VSAs, the system would support approximately 256K subscribers per SCE platform.
- Up to 20 subscriber attributes can be selected.

Note By default, the SCE platform converts the **3GPP-SGSN-Address-Code-6** VSA sent by Gx to **3GPP-SGSN-Address** VSA. Therefore, when using the SGSN address, both these attributes should be selected. The same behavior applies to the GGSN address VSA pair (**3GPP-GGSN-Address-Code-7** and **3GPP-GGSN-Address)**.

Capturing Subscriber Attributes Using the SCE

Capturing Subscriber Attributes

Attributes are received only from the Gx interface. The attributes selected by the CLI command are stored in the local attribute table and also copied to the SM. Any time one of these attributes is input for a subscriber by Gx, it is stored in the subscriber database for that subscriber.

When an attribute is deleted from the attribute table, all the entries for that attribute are also removed from the subscriber database.

Transmitting Subscriber Attributes

Attributes are transmitted only on the Gy interface. Three modes of output are supported:

- Always—Output the subscriber attributes on all the messages.
- On-change—Output the subscriber attributes any time a change is detected in at least one of the attributes.
- On-initial (default)—Output the subscriber attributes only on the first Gy message.

Subscriber Attribute CLI Commands

Table 6-1 lists the CLI commands used to configure and monitor the capture and sending of subscriber attributes.

Table 6-1 Subscriber Attribute CLI Commands

CLI Commands	Description
sub-attribute add-attribute <*attribute-name*>	Configure the capture of the specified attribute. Up to 20 subscriber attributes can be captured. The attribute name is selected from the list of VSAs with auto completion.
no sub-attribute <*attribute-name*>	Stop capturing the specified attribute and remove the entry from the attribute table. Also remove entries for the specified attribute from the subscriber database.
no sub-attribute all	Stop capturing all the VSA attributes and clear both the attribute table and the subscriber database.
show sub-attribute dictionary <*attribute-name*>	Show the entry in the dictionary table for the specified attribute.
show sub-attribute dictionary	Show the complete dictionary table.
show sub-attribute configuration	Show the attribute table, which contains the attributes currently selected to be captured, as well as the information from the attribute dictionary for each one.

Table 6-1 Subscriber Attribute CLI Commands (continued)

CLI Commands	Description
diameter Gy send-attributes (on-initial | on-change | always)	Configure when to transmit subscriber attributes.
no diameter Gy send-attributes	Disable transmitting subscriber attributes.

Example for showing the VSA dictionary:

```
show sub-attribute dictionary

     VSA name                        Vendor-ID  Attr-ID  Data Type   Protocol Interfaces
------------------------------------------------------------------------------------------
Acct-Multi-Session-ID                    -          50    UTF8String   Radius
Acct-Session-ID                          -          44    UTF8String   Radius
Acct-Session-Time                        -          46    Uint32       Radius
Called-Station-ID                        -          30    OCTETString  Radius
Calling-Station-ID                       -          31    OCTETString  Radius
Class                                    -          25    OCTETString  Radius
CUI                                      -          89    UTF8String   Diameter
Framed-IP-Address                        -           8    Address      Radius
NAS-Identifier                           -          32    OCTETString  Radius
NAS-IP-Address                           -           4    Address      Radius
NAS-Port-Type                            -          61    Uint32       Radius
User-Name                                -           1    OCTETString  Radius
User-Equipment-Info-Type                 -         459    Uint32       Diameter
User-Equipment-Info-Value                -         460    OCTETString  Diameter
3GPP-Charging-Characteristics            10415      13    UTF8String   Diameter
3GPP-Charging-Gateway-Address            10415       4    Address      Diameter
3GPP-Charging-ID                         10415       2    Uint32       Diameter
3GPP-GGSN-Address-Code-7                 10415       7    Address      Diameter
3GPP-GGSN-Address                        10415     847    Address      Diameter
3GPP-GGSN-MCC-MNC                        10415       9    UTF8String   Diameter
3GPP-GPRS-Negotiated-QoS-Profile         10415       5    UTF8String   Diameter
3GPP-IMEISV                              10415      20    UTF8String   Diameter
3GPP-IMSI                                10415       1    UTF8String   Diameter
3GPP-MS-Timezone                         10415      23    OCTETString  Diameter
3GPP-NSAPI                               10415      10    UTF8String   Diameter
3GPP-PDP-Type                            10415       3    Uint32       Diameter
3GPP-RAT-Type                            10415      21    OCTETString  Diameter
3GPP-Selection-Mode                      10415      12    UTF8String   Diameter
3GPP-SGSN-Address-Code-6                 10415       6    Address      Diameter
3GPP-SGSN-Address                        10415    1228    Address      Diameter
3GPP-SGSN-MCC-MNC                        10415      18    UTF8String   Diameter
3GPP-User-Location-Info                  10415      22    OCTETString  Diameter
CG-Address                               10415     846    Address      Diameter
WiMax-Active-Time                        24757      39    Uint32       GTP-C
WiMax-BSID                               24757      46    UTF8String   GTP-C
Sub-OS-Info-Map                          9        1071    UTF8String   Diameter
3GPP2-Home-Agent-IP-Address              5535        7    Address      Diameter
3GPP2-ESN                                5535       52    OCTETString  Diameter
3GPP2-MEID                               5535      116    OCTETString  Diameter
3GPP2-BSID                               5535       10    OCTETString  Diameter
3GPP2-IP-Technology                      5535       22    Uint32       Diameter
3GPP2-PCF-IP-Address                     5535        9    Address      Diameter
```

Example for selecting a VSA to capture and then showing the attribute configuration.

```
sub-attribute add-attribute 3GPP-Charging-Characteristics
do show sub-attribute configuration

     VSA name                        Vendor-ID  Attr-ID  Data Type   Protocol Interfaces
-----------------------------------------------------------------------------------------
3GPP-Charging-Characteristics          10415      13     UTF8String   Diameter  Gx
```

Capturing Subscriber Attributes Using the RADIUS LEG

A LEG usually listens to signaling data and provisions subscriber-based attributes. The SCE supports RADIUS Listener and Sniffer LEGs. The subscriber attributes are configurable and customizable in the SM. The LEGs are responsible for providing the configured data to the SM and the SM provisions the data to the SCE platform.

RADIUS Sniffer LEG

Capturing subscriber attributes using the RADIUS sniffer LEG works as follows:

1. The user configures the set of subscriber attributes to extract (up to 20), which are provisioned to the RADIUS sniffer module in the SCE.
2. When the SCE detects a RADIUS accounting message, it extracts the attributes from the message and sends it to the SM in the RADIUS/Login RDR.
3. The RADIUS Sniffer LEG in the SM receives the RADIUS RDR and stores the attribute values in its local database.
4. The SM updates the subscriber attribute table in the SCE with the subscriber attributes learned.

Note The RADIUS sniffer module can be in a different SCE platform from the one that processes the traffic.

RADIUS Listener LEG

Capturing subscriber attributes using the RADIUS Listener LEG works as follows:

1. The user configures the set of subscriber attributes to extract (up to 20).
2. The RADIUS Listener LEG listens to RADIUS accounting messages received in the SM and extracts the attributes configured.
3. The RADIUS Listener LEG in the SM stores the attribute values in its local database.
4. The SM updates the subscriber attribute table in the SCE with the subscriber attributes learned.

Configuring the Attributes to Be Captured

You specify which subscriber attributes to capture by editing the relevant configuration file:

- RADIUS Listener LEG configuration file is at **sm-inst-dir/sm/server/root/config/p3sm.cfg**
- RADIUS Sniffer LEG configuration file is at **sm-inst-dir/sm/server/root/config/rad_snif.cfg**

Note For more information about configuring the RADIUS LEGs, see the *Cisco SCMS SM LEGs User Guide*.

For each attribute you want the LEG to capture, add a section to the appropriate configuration file, as follows:

[Radius.Field.Attribute_name]

radius_attribute = <ID> [(<radius_attribute_vendor_id>, <radius_sub_attribute>)]

radius_attribute_type = <type>

Table 6-2 [Radius.Field.] Field Descriptions

Field	Description
Attribute_name	Name of the attribute to be captured.
ID	Attribute ID. If the attribute is a VSA, the ID is set to 26 and the attribute vendor ID and subattribute are set as well. If the attribute is not a VSA, enter the ID (there is no default). The attribute vendor ID and sub-attribute fields are not used.
radius_attribute_vendor_id	Set when the attribute is a VSA.
radius_sub_attribute	Set when the attribute is a VSA.
type	Attribute type. Possible values are string or integer. There is no default value.

This example shows how to edit the configuration file to add the 3GPP-SGSN-Address (VSA) attribute:

```
[Radius.Field.3GPP-SGSN-Address]
radius_attribute = 26(10415;6)
radius_attribute_type = integer
```

Provisioning the SCE with SM Subscriber Attributes

When the SM (RADIUS LEG) captures the subscriber attributes, it provisions them to the SM over the SM-SCE API. The SM provides a list of attributes with the following information for each attribute:

- Attribute code. If attribute is a VSA, this is the VSA code.
- Flags. One bit indicates whether this is a VSA.
- Attribute vendor ID (if attribute is a VSA).
- Attribute-type
- Attribute length
- Attribute value

If the SM attribute definition (type, size, and so on) does not match the SCE attribute definition, the attribute is discarded, and an appropriate error message is sent.

Note The SCE copies into its local database only the attributes from the 20 attributes configured in the SCE and present in the SCE database, regardless of what attributes are defined to be reported in the RDRs.

Generating Mobile Reports

Subscriber attributes that have been captured by either the SCE or the SM can be used to generate mobile reports. The subscriber attributes are appended to the RDRs and sent to the CM, where the reports are generated.

Use a mediation data warehouse device for full flexibility and long period granular data.

Appending Subscriber Attributes to SCE RDRs

SCE provides subscriber attributes as part of the following RDRs:

- Subscriber Usage RDR (TAG: 4042321920)
- HTTP Transaction Usage RDR (TAG: 4042323004)
- Video Transaction Usage RDR (TAG: 4042323072)

You can enable or disable reporting subscriber attributes in these RDRs either from the SCA BB console or by a CLI command.

Table 6-3 Subscriber Attributes Reported in RDRs

Attribute	Type	Max Size [B]	Attribute ID	VSA	Vendor-ID
Acct-Multi-Session-ID	String	32	50	N	
Acct-Session-ID	String	253	44	N	
Framed-IP-Address	Address	4	8	N	
Called-Station-ID	String	253	30	N	
3GPP-IMEISV	String	16	20	Y	10415
3GPP-IMSI	String	15	1	Y	10415
3GPP-RAT-Type	String	1	21	Y	10415
3GPP-SGSN-Address	Address	4	6	Y	10415
3GPP-SGSN-MCC-MNC	String	6	18	Y	10415
3GPP-User-Location-Info	String	253	22	Y	10415
WiMax-BSID	String	30	46	Y	24757
3GPP2-MEID	String	—	116	Y	5535
3GPP2-ESN	String	—	52	Y	5535
3GPP2-PCF-IP-Address	Address	4	9	Y	5535
3GPP2-Home-Agent-IP-Address	Address	4	7	Y	5535

General Information:

- The SCE reports in the RDRs only the attributes which exist in its local database.
- If an attribute defined for the RDR is not in the database, the attribute is appended to the RDR with a NULL value.

- The attributes structure in the RDR is constant, with each attribute always at the same location, and appearing in the order that they appear in Table 6-3.
- The format of the attributes in the RDR is the same as the "type" specified in the RADIUS attribute (integer or string).

Control Field

A control field is defined in the RDR providing the following information:

- Indicating that subscriber attributes are appended
- SPECIFYING which of the attributes in the message are valid

The control field comes after the original RDR parameters and before the first VSA data.

Each bit in the control field corresponds to one of the subscriber attributes listed in Table 6-3. Bit "0" corresponds to Acct-Multi-Session-ID, bit "1" corresponds to Acct-Session-ID, and bit "10" corresponds to WiMax-BSID.

Value 0 means that the data is not present, and value 1 means that data pertaining to the corresponding VSA is present and valid. See the control fields provided in the two examples in "Examples: Reporting the Subscriber Attributes in Enabled RDRs" section on page 6-9.

Configuring Reporting Subscriber Attributes in RDRs from the SCE

Table 6-4 Reporting Subscriber Attributes in RDR CLI Command

CLI Commands	Description
rdr-formatter sub-attribute send-attributes	Enable reporting subscriber attributes in RDRs.
no rdr-formatter sub-attribute send-attributes	Disable reporting subscriber attributes in RDRs

Examples: Reporting the Subscriber Attributes in Enabled RDRs

Subscriber usage RDR with all 15 VSA fields presented:

```
#4042321920:
rdrParty       // Subscriber ID
10             // Package ID
1              // Service Usage counter ID
0              // Breach State
1              // Reason
60             // Configured Duration
60             // Duration
1275330073     // End Time
100            // Upstream Volume
100            // DownStream Volume
5              // Sessions
5              // Seconds
1              // Up VLink
1              // Down VLink
32767          // Control Field (0b111111111111111) (15 fields enabled)
Subscriber1    // Acct-Multi-Session-ID   (bit 0)
lkjhgfdsa      // Acct-Session-ID         (bit 1)
10.1.2.3       // Framed IP Address       (bit 2)
abcdefg        // Called Station ID       (bit 3)
000000000000   // 3GPP-IMEISV             (bit 4)
000000100000   // 3GPP-IMSI               (bit 5)
700300100050   // 3GPP-RAT-Type           (bit 6)
10.1.1.1       // 3GPP-SGSG-Address       (bit 7)
```

```
mhutexcfvkli   // 3GPP-SGSN-MCC-MNC       (bit 8)
abc            // 3GPP-User-Location-Info (bit 9)
3p3p3          // WiMax-BSID              (bit 10)
A0000020D92AAA // 3GPP2-MEDI                  (bit 11)
80dc47ed       // 3GPP2-ESN                   (bit 12)
10.222.202.5   // 3GPP2-PCF-IP-Address        (bit 13)
68.28.57.76    // 3GPP2-home-Agent-IP-Address (bit 14)
```

Subscriber usage RDR with partial VSA fields presented:

```
#4042321920:
rdrParty       // Subscriber ID
10             // Package ID
1              // Service Usage counter ID
0              // Breach State
1              // Reason
60             // Configured Duration
60             // Duration
1275330073     // End Time
100            // Upstream Volume
100            // DownStream Volume
5              // Sessions
5              // Seconds
1              // Up VLink
1              // Down VLink
27541           // Control Field (0b110101111111001 - Acct-Session-ID, Framed IP Address,
                    WiMax-BSID, and 3GPP2-ESN are not valid)
Subscriber1    // Acct-Multi-Session-ID   (bit 0)
               // Acct-Session-ID         (bit 1)
0              // Framed IP Address       (bit 2)
abcdefg        // Called Station ID       (bit 3)
000000000000   // 3GPP-IMEISV             (bit 4)
000000100000   // 3GPP-IMSI               (bit 5)
700300100050   // 3GPP-RAT-Type           (bit 6)
10.1.1.1       // 3GPP-SGSG-Address       (bit 7)
mhutexcfvkli   // 3GPP-SGSN-MCC-MNC       (bit 8)
abc            // 3GPP-User-Location-Info (bit 9)
               // WiMax-BSID              (bit 10)
A0000020D92AAA // 3GPP2-MEDI                  (bit 11)
               // 3GPP2-ESN                   (bit 12)
10.222.202.5   // 3GPP2-PCF-IP-Address        (bit 13)
68.28.57.76    // 3GPP2-home-Agent-IP-Address (bit 14)
```

Configuring Reporting Subscriber Attributes in RDRs from the SCA BB Console

You can enable appending VSA fields in RDRs from the SCA BB console.

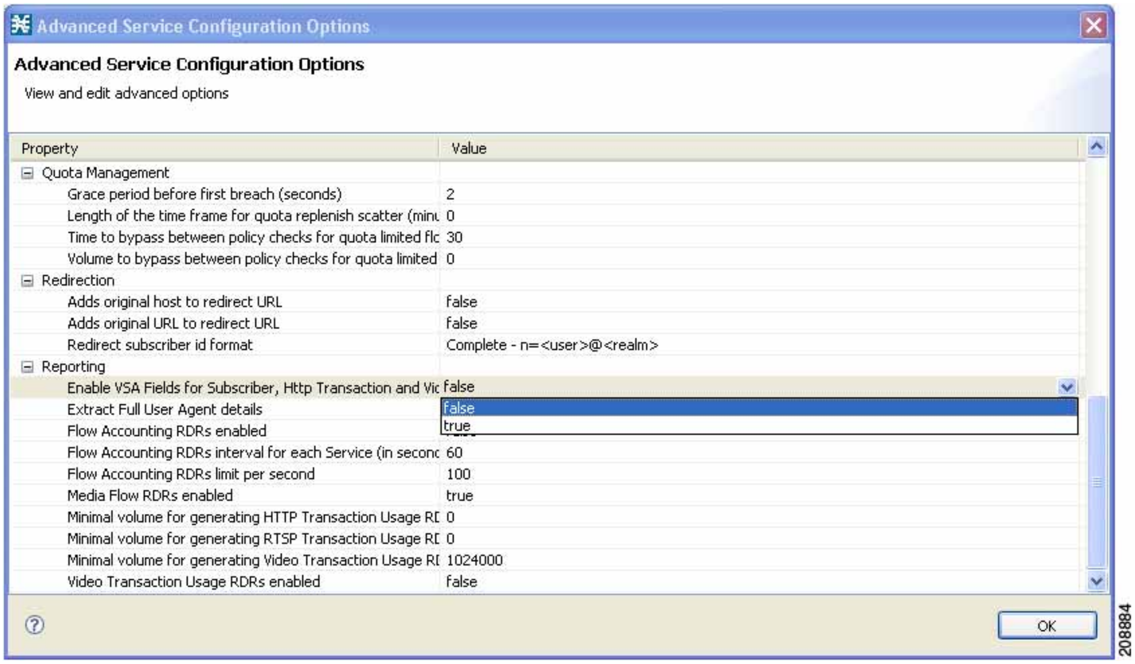
Step 1 Choose **Configuration** > **Policies** > **System Settings** > **Advanced Options**.

Step 2 Click **Advanced Service Configuration Options**.

Step 3 Scroll down to the **Reporting** section.

Step 4 Set the value of 'Enable VSA Fields for Subscriber, HTTP Transaction, and Video Transaction RDRs' (first line) to '**True**'. (See Figure 6-2.)

Figure 6-2 Enabling VSA Fields in RDRs


Advanced Service Configuration Options
Advanced Service Configuration Options
View and edit advanced options
OK
208884

Property	Value
⊟ Quota Management	
Grace period before first breach (seconds)	2
Length of the time frame for quota replenish scatter (minu	0
Time to bypass between policy checks for quota limited flc	30
Volume to bypass between policy checks for quota limited	0
⊟ Redirection	
Adds original host to redirect URL	false
Adds original URL to redirect URL	false
Redirect subscriber id format	Complete - n=<user>@<realm>
⊟ Reporting	
Enable VSA Fields for Subscriber, Http Transaction and Vic	false false true
Extract Full User Agent details	
Flow Accounting RDRs enabled	
Flow Accounting RDRs interval for each Service (in seconc	60
Flow Accounting RDRs limit per second	100
Media Flow RDRs enabled	true
Minimal volume for generating HTTP Transaction Usage RI	0
Minimal volume for generating RTSP Transaction Usage RI	0
Minimal volume for generating Video Transaction Usage RI	1024000
Video Transaction Usage RDRs enabled	false

Step 5 Click **OK**.

Step 6 Click **OK** in the System Settings dialog box.

.

Supported Mobile Reports

The following information is derived from specific attributes sent to the CM in RDRs and used to generate mobile reports:

- Device type:
  - RADIUS device type—Located as part of the 3GPP-IMEI (RADIUS attribute 20)
  - Diameter device type—Encoded in the User-Equipment-Info AVP (code 458)
- APN—Mapped from the RADIUS/Diameter Called-Station-ID field
- User location—Mapped from 3GPP-User-Location-Information
- Network type—Mapped from 3GPP-RAT-Type

Based on the above attributes, the common mobile reports are generated in the CM/Reporter (see Table 6-5). Examples of some of the reports that can be generated are displayed in the "Mobile Report Examples" section on page 6-13.

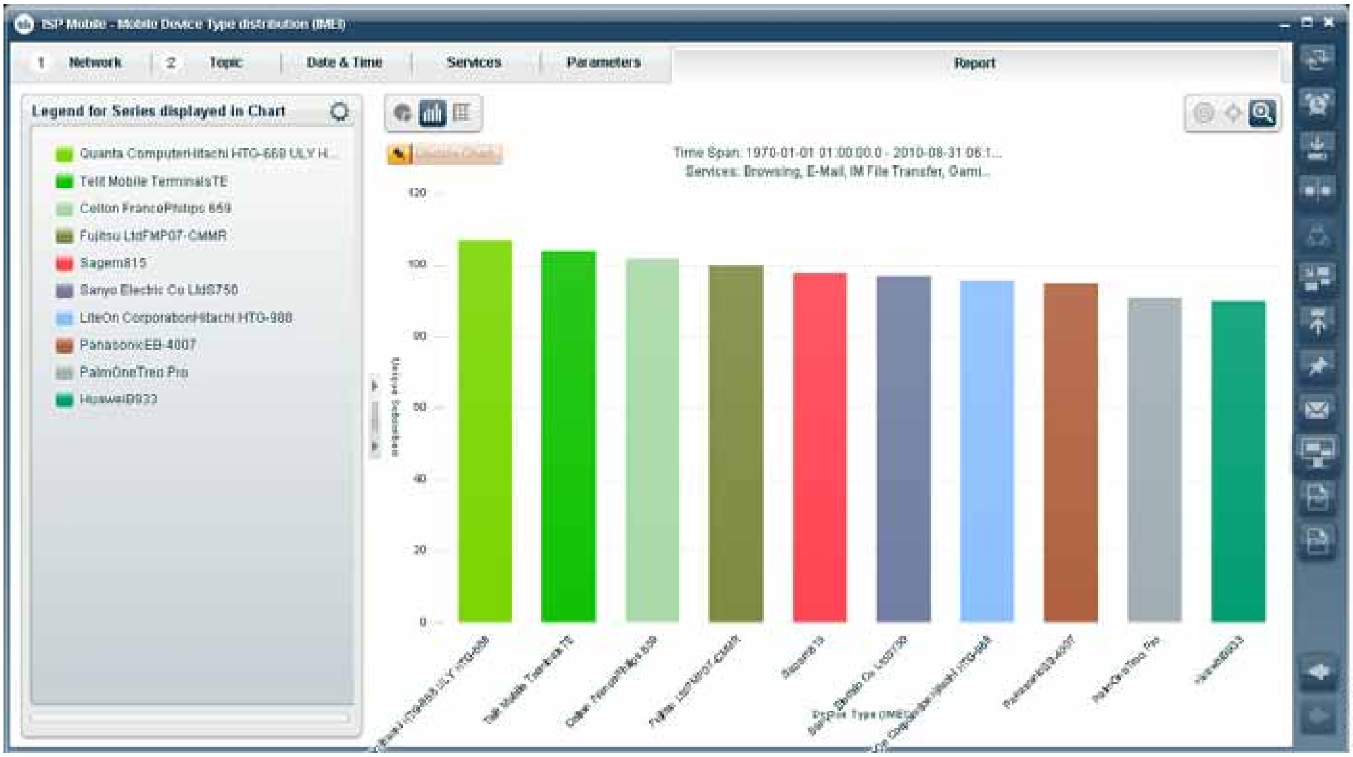
Table 6-5 List of Mobile Reports

Report	X	Y	Filters
Device Type Distribution (IMEI)	Device Type (IMEI)	Number of unique subscribers per device type	Time window, Top devices
Usage per device type	Device Type (IMEI)	Total usage per device	Time window, Top usage
Application usage for specific device	Time	Application usage	Time window
Usage Per Network Type	Network Type	Total usage per network	Time window, Top networks
Application usage for specific network type	Time	Application usage	Time window
Usage per APN	APN Name	Total usage per APN	Time window, Top APNs
Application Usage for Specific APN	Time	Application usage	Time window
Number of subscribers per location	Time	Number of subscribers	Time-based
Usage per location	Location ID	Total usage for location	Time-based, Top locations
Usage per SGSN	SGSN	Total usage for SGSN type	Time-based, Top SGSNs

Mobile Report Examples

Device Type Distribution

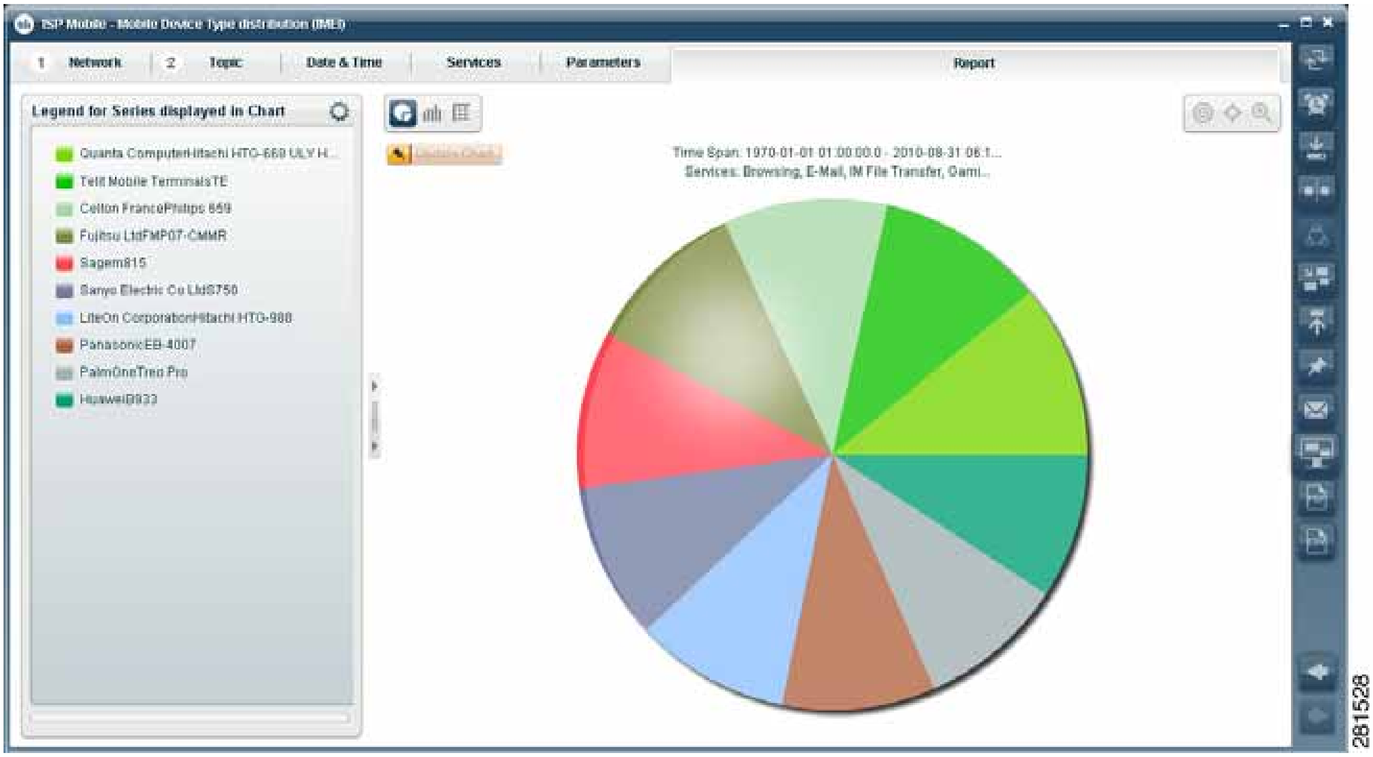
Figure 6-3 Device Type Distribution by Unique Subscribers (bar)


ISP Mobile - Mobile Device Type distribution (IMEI)
1 Network
2 Topic
Date & Time
Services
Parameters
Report
Legend for Series displayed in Chart
🟩 Quanta ComputerHitachi HTG-669 ULY H...
🟩 Telit Mobile TerminalsTE
🟩 Celton FrancePhilips 659
🟫 Fujitsu LtdFMP07-CMMR
🟥 Sagem815
🟪 Sanyo Electric Co LtdS750
🟦 LiteOn CorporationHitachi HTG-988
🟫 PanasonicEB-4007
⬜ PalmOneTreo Pro
🟩 HuaweiB933
Unique Subscribers
120
100
80
60
40
20
0
Device Type (IMEI)

Time Span: 1970-01-01 01:00:00.0 - 2010-08-31 06:1...
Services: Browsing, E-Mail, IM File Transfer, Gami...

281527

Figure 6-4 Device Type Distribution by Unique Subscribers (pie)


ISP Mobile - Mobile Device Type distribution (IMEI)
1 Network
2 Topic
Date & Time
Services
Parameters
Report
Legend for Series displayed in Chart
🟩 Quanta ComputerHitachi HTG-660 ULY H...
🟩 Telit Mobile TerminalsTE
🟩 Celton FrancePhilips 659
🟫 Fujitsu LtdFMP07-CMMR
🟥 Sagem815
🟪 Sanyo Electric Co LtdS750
🟦 LiteOn CorporationHitachi HTG-988
🟫 PanasonicEB-4007
⬜ PalmOneTreo Pro
🟩 HuaweiB933
Update Chart
281528

Time Span: 1970-01-01 01:00:00.0 - 2010-08-31 06:1...
Services: Browsing, E-Mail, IM File Transfer, Gami...

Usage Per Network Type

Figure 6-5 Usage per Network Type (bar)

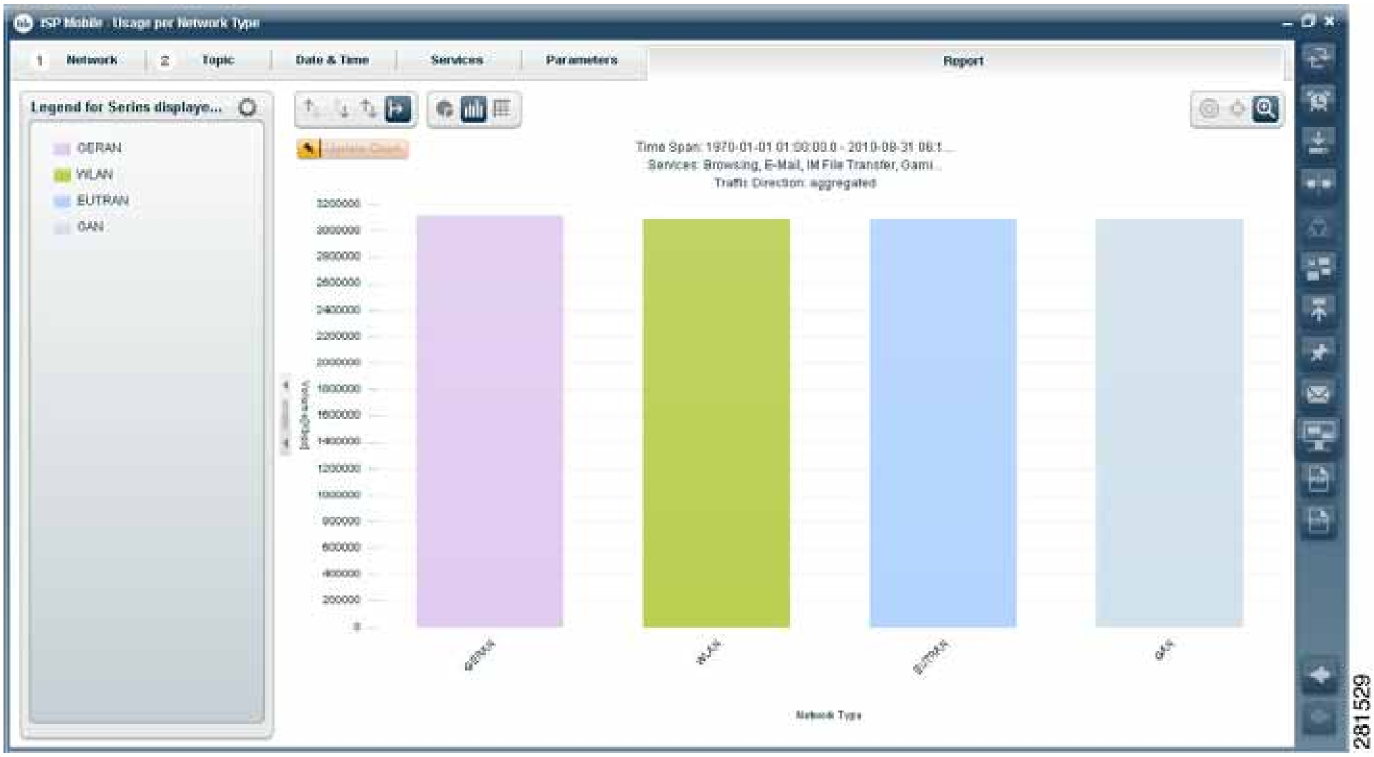
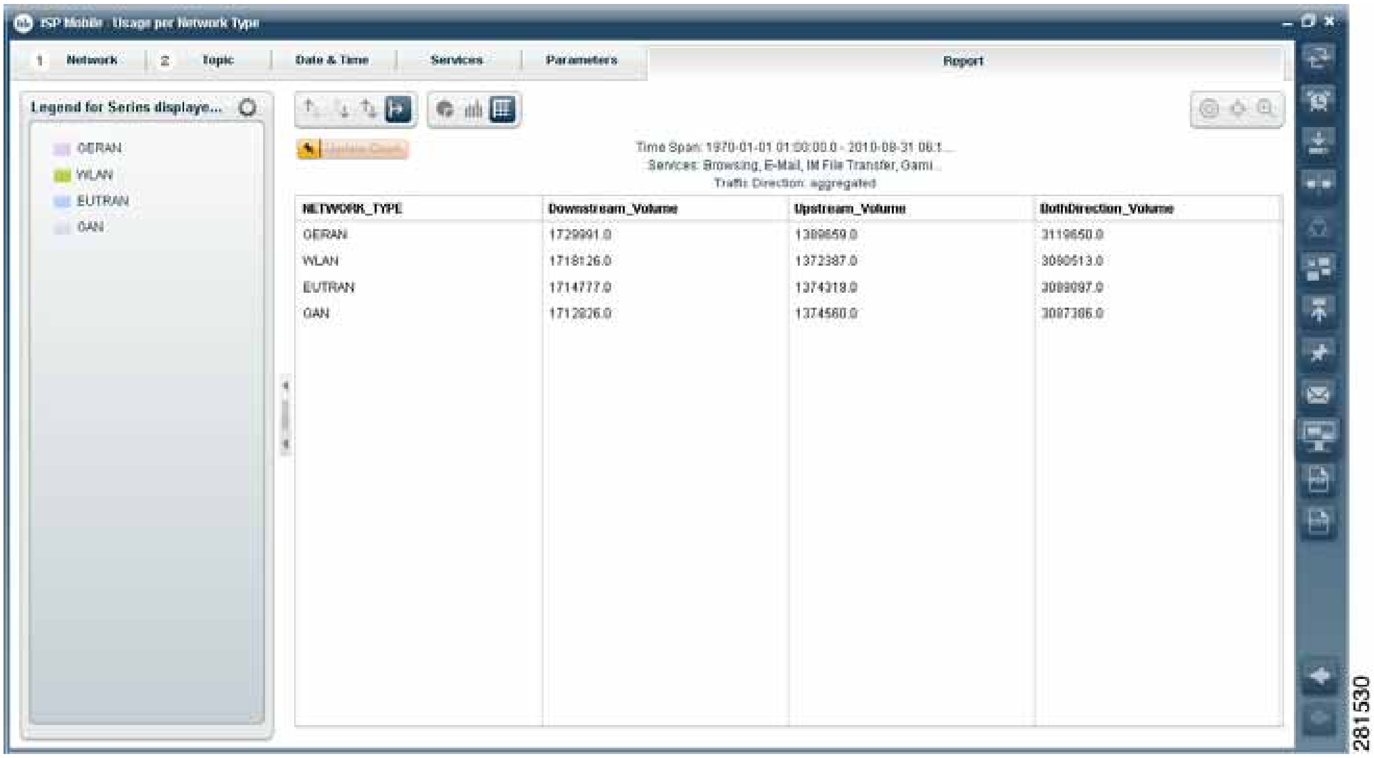


Figure 6-6 Usage per Network Type (table)

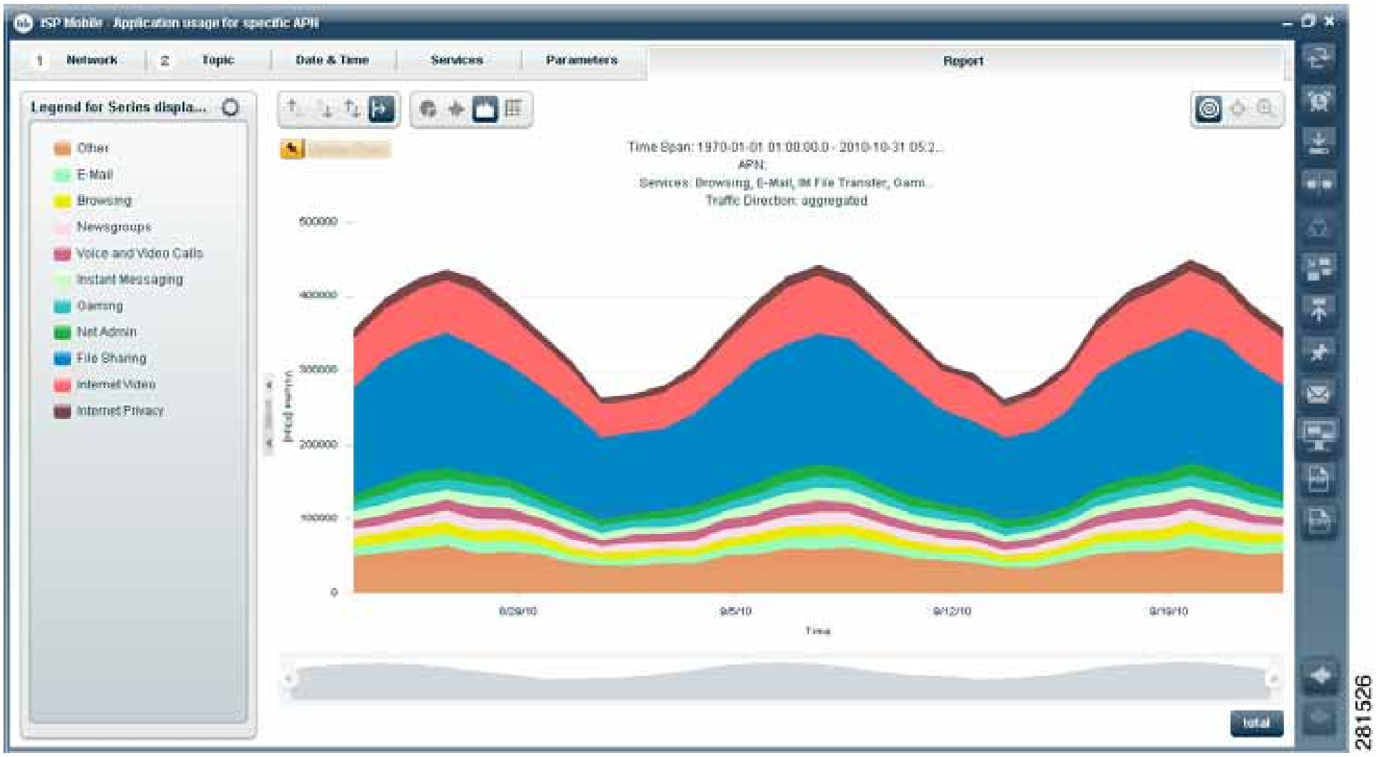


Time Span: 1970-01-01 01:00:00.0 - 2010-08-31 08:1...
Services: Browsing, E-Mail, IM File Transfer, Gami...
Traffic Direction: aggregated

NETWORK_TYPE	Downstream_Volume	Upstream_Volume	BothDirection_Volume
GERAN	1729991.0	1389659.0	3119650.0
WLAN	1718126.0	1372387.0	3090513.0
EUTRAN	1714777.0	1374319.0	3089097.0
GAN	1712826.0	1374560.0	3087386.0

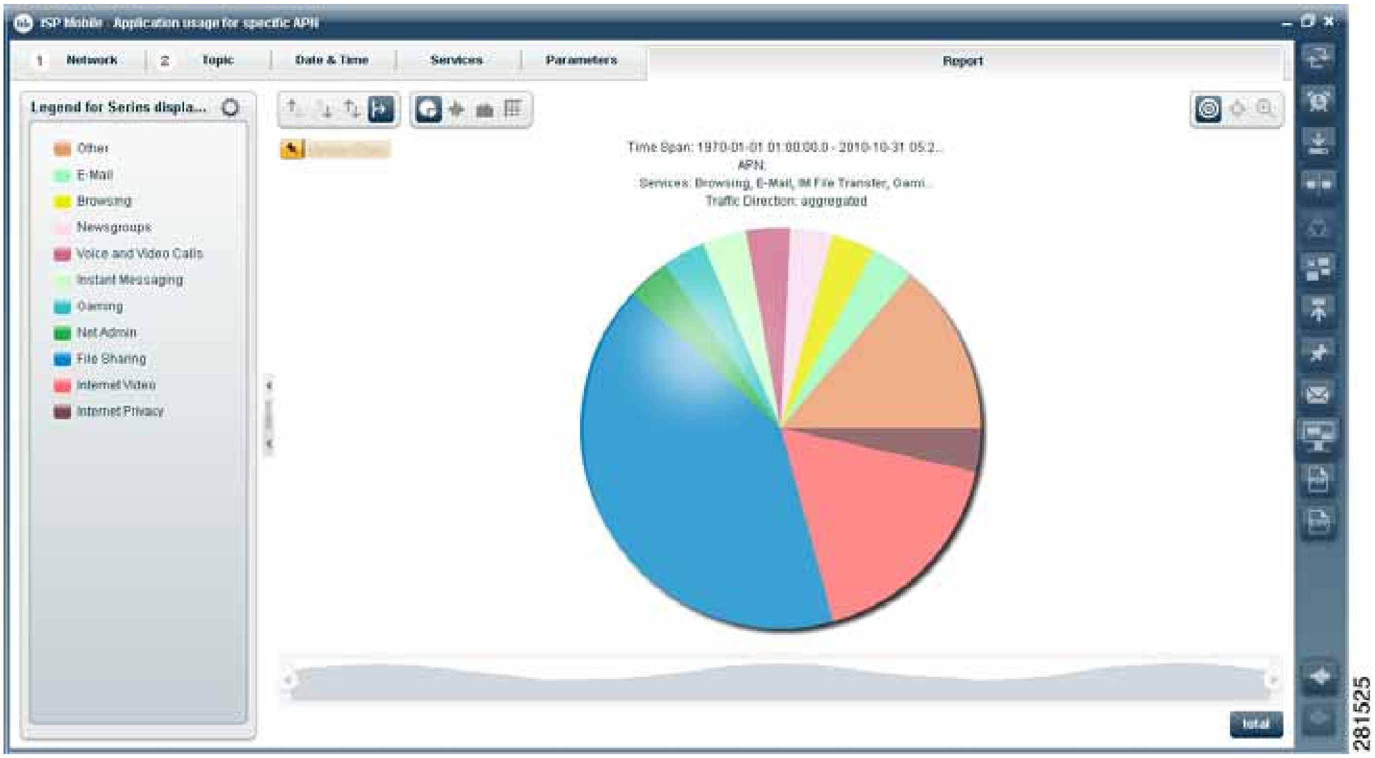
Application Usage for Specific APN

Figure 6-7 Application Usage for Specific APN (stacked area)



Time Span: 1970-01-01 01:00:00.0 - 2010-10-31 05:2...
APN:
Services: Browsing, E-Mail, IM File Transfer, Gami...
Traffic Direction: aggregated

Figure 6-8 Application Usage for Specific APN (pie)



Time Span: 1970-01-01 01:00:00.0 - 2010-10-31 05:2...
APN:
Services: Browsing, E-Mail, IM File Transfer, Gami...
Traffic Direction: aggregated

APPENDIX A

Supported Message Formats

Revised: July 24, 2012, OL-24167-04

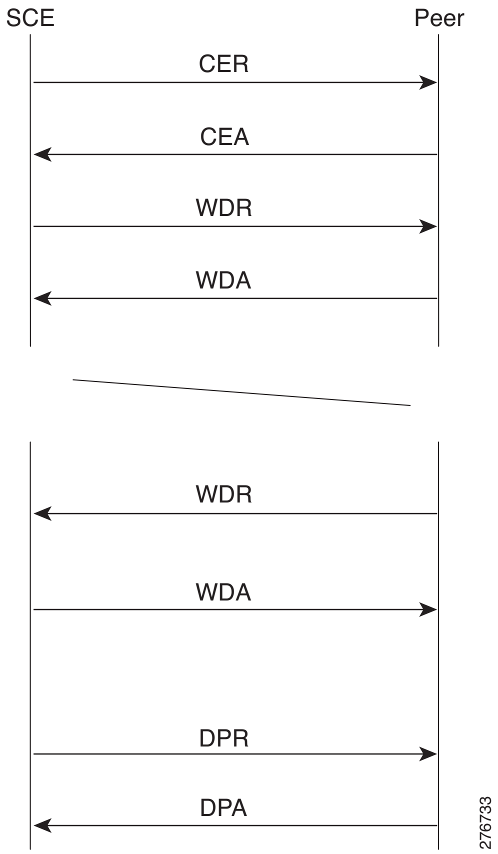
Supported Diameter Messages

The messages sent and received by the diameter infrastructure are as follows:

- Capability Exchange Request (CER)—Sent upon new connection establishment from the SCE to peer. The main purpose of this message is to advertise which applications are supported by peers. It also includes some other details such as realm, host, and so on.
- Capability Exchange Answer (CEA)—Responds to the CER message.
- Watch Dog Request (WDR)—Sent by one peer to another. The purpose is to ensure that the connection is up and running. If three watch dog messages in a row are not answered, the connection is closed and reopened, and only after three messages are answered will it be considered up.
- Watch Dog Answer (WDA)—Responds to WDR message.
- Disconnect Peer Request (DPR)—Tells the peer that the connection will be disconnected.
- Disconnect Peer Answer (DPA)—Responds to the DPR message.

Figure A-1 displays the typical connection flow of diameter messages and responses.

Figure A-1 Typical Connection Flow



The SCE initiates the TCP connection (the only transport layer currently supported by SCE). After the TCP connection is established, the SCE sends the CER message. The CER message is answered by the CEA message. At this stage the connection is up. The WDR and WDA messages are exchanged between the peers. The time gap between watch dog messages is defined by the Tx timer. If the peer is removed, the connection is gracefully closed by sending the DPR message and receiving the DPA message.

Gx-Supported Messages

The following messages are supported:

- Credit Control Request (CCR)—The CCR message indicates Gx diameter session create, update, and close.

  CCR Initiate is sent by the SCE to the PCRF (Gx Server) upon login of a subscriber (for example, using SceSubsciberAPI) or upon new flow mapped to a Gx anonymous group. Upon login, the CCR includes parameters that identify the subscriber to the PCRF, such as Framed-ip and Subscription-Id (not on anonymous-group).

  CCR Terminate is sent on logout.
- Credit Control Answer (CCA)—A CCA message is sent from the server to the SCE.
  - Responding to a CCR Initial request—The CCA message includes the subscriber policy parameters and RADIUS VSA attributes (or some subset of it).
  - Responding to a CCR Terminate request—The CCA message generally includes only results of the action.
- Re-Authorize Request (RAR)—A RAR message is initiated by the PCRF. The RAR message can include new parameters (package, and so on) and RADIUS VSA attributes. The RAR message is initiated by an external event.
- Re-Authorize Answer (RAA)—A RAA message is the response to the RAR. It usually includes the result of the action.
- Abort Session Request (ASR)—An ASR message is sent from the PCRF to the SCE to close the subscriber session, and in some cases to trigger a logout of the subscriber. A subscriber owned by a Gx (anonymous group manager), is logged out.
- Abort Session Answer (ASA)—An ASA message is the response to ASR message and usually contains the result of the action.

Credit Control Request (CCR)

Command-Code Field	Command Flags Field	Direction	Description
272	'R' bit set	SCE to PCRF	Sent to: • Request SCE rules for a subscriber • Indicate termination of the subscriber

Message Format:

```
<CC-Request> ::= < Diameter Header: 272, REQ, PXY >
                < Session-Id >
                { Auth-Application-Id }
                { Origin-Host }
                { Origin-Realm }
                { Destination-Realm }
                { CC-Request-Type }
                { CC-Request-Number }
                [ Destination-Host ]
                [ Framed-IP-Address ]
                [ Subscription-Id ]
```

The format of the Session-Id is `"pid; ip; time"`, where:

- PID is a 32-bit integer type indicating the unique PID for a specific Gx session.
- IP is a 32-bit unsigned integer type indicating the framed IP of the subscriber for which the session is created. IP is in decimal format.

TIME is a 32-bit unsigned integer type indicating the time when session is created. Time is in number of seconds starting from January 1, 1970.

Message Response:

- Auth-Application-Id is set to the application ID of the Gx protocol.
- Origin-Host is set to the SCE host id (its IP).
- Origin-Realm is set to “SCE” defined realm.
- Destination-Host and Destination-Realm define the PCRF destination. The destination host is not mandatory, it depends on the SCE and PCRF configurations.
- CC-Request-Type is set to “Initial” on session creation (SCE login) and “Termination” on session termination (SCE logout).
  CC-Request-Number is a unique number within a session-id.
- Framed-IP-Address and Subscription-Id will be sent depending on the scenario.

Case 1: Login mode

- The CCR includes both parameters.
- Framed-IP-Address is the IP address of the subscriber. (Will not be sent on “TERMINATE”.)
- Subscription-Id is set to the subscriber-ID used by the SCE (for example, IMSI/MSISDN).
- The subscription-Id will be introduced to the SCE by a different API.

Case 2: Pull mode

- The CCR includes only the Framed-IP-Address AVP. The subscription-Id is returned as part of the CCA.
- Framed-IP-Address is the IP address of the subscriber.
- In this mode, the Gx interface is also used to introduce the subscribers to the SCE.

Sample Message Login mode:

```
Version        = 1
Message Length = XXX
Command Flags  = REQ, PXY
Command Code   = Credit-Control-Request (272)
Application Id = 16777238
AVPs
    Session-Id             = "27; 3232262425; 1311857000"
    Auth-Application-Id    = 16777238
    Origin-Host            = "10.101.23.34"
    Origin-Realm           = "sce"
    Destination-Realm      = "att.com"
    Destination-Host       = "PCRF host"
    CC-Request-Type        = INITIAL_REQUEST (1)
    CC-Request-Number      = 0
    Framed-IP-Address      = 10.10.1.10
    Subscription-Id        = 05412345566
```

Sample Message Pull mode:

```
Version        = 1
Message Length = XXX
Command Flags  = REQ, PXY
Command Code   = Credit-Control-Request (272)
Application Id = 16777238
AVPs
    Session-Id         = "27; 3232262425; 1311857000"
    Auth-Application-Id= 16777238
    Origin-Host        = "10.101.23.34"
    Origin-Realm       = "sce"
    Destination-Realm  = "att.com"
    Destination-Host   = "PCRF host"
    CC-Request-Type    = INITIAL_REQUEST (1)
    CC-Request-Number  = 0
    Framed-IP-Address  = 10.10.1.10
```

The format of the Session-Id is `“pid; ip; time”`, where:

- PID is a 32-bit integer type indicating the unique PID for a specific Gx session.
- IP is a 32-bit unsigned integer type indicating the framed IP of the subscriber for which the session is created. IP is in decimal format.

TIME is a 32-bit unsigned integer type indicating the time when session is created. Time is in number of seconds starting from January 1, 1970.

Credit Control Answer (CCA)

The CCA command has two formats:

- CCA Initial
- CCA Update/Terminate

Command-Code Field	Command Flags Field	Direction	Description
272	'R' bit cleared	PCRF to SCE	Sent in response to the CCR command. Used to provision SCE rules and event triggers for the subscriber.

CCA Initial

Message Format:

```
<CC-Answer> ::= < Diameter Header: 272, PXY >
                < Session-Id >
                { Auth-Application-Id }
                { Origin-Host }
                { Origin-Realm }
                { CC-Request-Type }
                { CC-Request-Number }
                { Subscription-Id }
                   [ Subscription-Id-Type ]
                   [ Subscription-Id_Data ]
                [ Result-Code ]
                [ Cisco-SCA BB-Package-Install ]
                [ Cisco-SCA BB-Package-Install ]
                [ Cisco-SCA BB-Real-time-monitor-Install ]
                [ Cisco-SCA BB-Vlink-Upstream-Install ]
                [ Cisco-SCA BB-Vlink-Downstream-Install ]
                [ PS-Information ]
                    [3GPP-GGSN-Address]
                    [3GPP-SGSN-Address]
                   [CG-Address]
                    [3GPP-Charging-Id]
                    [Called-Session-Id]
                    [3GPP-GPRS-QoS-Negotiated-Profile]
                    [3GPP-PDP-Type]
                    [3GPP-SGSN-MCC-MNC]
                    [3GPP-GGSN-MCC-MNC]
                    [3GPP-Charging-Characteristics]
                    [3GPP-RAT-Type]
                    [3GPP-Selection-Mode]
                    [3GPP-NSAPI]
                    [3GPP-MS-Timezone]
                    [3GPP-User-Location-Info]
                [Acct-Multi-Session-ID]
                [Acct-Session-ID]
                [Acct-Session-Time]
                [Calling-Station-ID]
                [Class]
                [CUI]
                [Framed-IP-Address]
                [NAS-Identifier]
                [NAS-IP-Address]
                [NAS-Port-Type]
                [User-Name]
                [3GPP-GGSN-Address-Code-7]
                [3GPP-IMEISV]
                [3GPP-IMSI]
                [3GPP-CG-Address]
                [3GPP-SGSN-Address-Code-6]
                [WiMax-Active-Time]
                [WiMax-BSID]
```

Message Response:

- Session-Id is set to the CCR Session-Id.
- Auth-Application-Id is set to the same value as the CCR.
- Origin-Host is set to the message generating host (PCRF which responds).
- Origin-Realm is set to the PCRF realm.

- CC-Request-Type and CC-Request-Number are set to the same type as in the CCR.
- Subscription-Id is set to the subscriber-ID used by the SCE.
- Cisco-SCA BB-Package-Install is set to the subscriber assigned package ID.
- Cisco-SCA BB-Real-time-monitor-Install is set to real monitor activation value.
- Cisco-SCA BB-Vlink-Upstream-Install is set to the upstream vlink assigned ID.
- Cisco-SCA BB-Vlink-Downstream-Install is set to the downstream vlink assigned ID.

For Login mode, only the Cisco-SCA BB-Package-Install is mandatory. For Pull mode, both Cisco-SCA BB-Package-Install and Subscription-Id are mandatory. Additional attributes are sorted and can be used by other interfaces, such as Gy.

Sample Message:

```
Version        = 1
Message Length = XXX
Command Flags  = PXY
Command Code   = Credit-Control-Answer (272)
Application Id = 16777238
AVPs
   Session-Id         = "27; 3232262425; 1311857000"
   Auth-Application-Id= 16777238
   Origin-Host        = "PCRF host"
   Origin-Realm       = "PCRF Realm"
   CC-Request-Type    = INITIAL_REQUEST (1)
   CC-Request-Number  = 0
   Subscription-Id    = 05412345566
      Subscription-Id-Type = END_USER_E164 (0)
      Subscription-Id-Value = 1110123456
   Result-Code        = DIAMETER_SUCCESS
   Cisco-SCA BB-Package-Install = 5
   Cisco-SCA BB-Real-time-monitor-Install = 1
```

The format of the Session-Id is `“pid; ip; time”`, where:

- PID is a 32-bit integer type indicating the unique PID for a specific Gx session.
- IP is a 32-bit unsigned integer type indicating the framed IP of the subscriber for which the session is created. IP is in decimal format.
- TIME is a 32-bit unsigned integer type indicating the time when session is created. Time is in number of seconds starting from January 1, 1970.

Error Handling

- If a timeout event occurs, or if a CCA is returned with an error code, the SCE tries to open the session again after 15 seconds, 30 seconds, 60 seconds, and then every 120 seconds.
- Rejection is not supported. To reject a subscriber, the PCRF must return a CCA with a success code that installs a special package used for this purpose.
- If the user is not recognized by the PCRF server, the PCRF should return a CCA with fail code and wait for retry. It is also possible to return a success code that installs the blocking\rejecting\limiting package, and update it later by using RAR, when the PCRF gets new information about the subscriber.

CCA Update/Terminate

Message Format:

```
<CC-Answer> ::= < Diameter Header: 272, PXY >
                < Session-Id >
                { Auth-Application-Id }
                { Origin-Host }
                { Origin-Realm }
                { CC-Request-Type }
                { CC-Request-Number }
                [ Result-Code ]
                [ Cisco-SCA BB-Package-Install ]
                [ Cisco-SCA BB-Package-Install ]
                [ Cisco-SCA BB-Real-time-monitor-Install ]
                [ Cisco-SCA BB-Vlink-Upstream-Install ]
                [ Cisco-SCA BB-Vlink-Downstream-Install ]
                [ PS-Information ]
                    [3GPP-GGSN-Address]
                    [3GPP-SGSN-Address]
                   [CG-Address]
                    [3GPP-Charging-Id]
                    [Called-Session-Id]
                    [3GPP-GPRS-QoS-Negotiated-Profile]
                    [3GPP-PDP-Type]
                    [3GPP-SGSN-MCC-MNC]
                    [3GPP-GGSN-MCC-MNC]
                    [3GPP-Charging-Characteristics]
                    [3GPP-RAT-Type]
                    [3GPP-Selection-Mode]
                    [3GPP-NSAPI]
                    [3GPP-MS-Timezone]
                    [3GPP-User-Location-Info]
                [Acct-Multi-Session-ID]
                [Acct-Session-ID]
                [Acct-Session-Time]
                [Calling-Station-ID]
                [Class]
                [CUI]
                [Framed-IP-Address]
                [NAS-Identifier]
                [NAS-IP-Address]
                [NAS-Port-Type]
                [User-Name]
                [3GPP-GGSN-Address-Code-7]
                [3GPP-IMEISV]
                [3GPP-IMSI]
                [3GPP-CG-Address]
                [3GPP-SGSN-Address-Code-6]
                [WiMax-Active-Time]
                [WiMax-BSID]
```

Message Response:

- Session-Id is set to the CCR Session-Id.
- Auth-Application-Id is set to the same value as the CCR.
- Origin-Host is set to the message generating host (PCRF which responds).
- Origin-Realm is set to the PCRF realm.
- CC-Request-Type and CC-Request-Number are set to the same type as in the CCR.
- Cisco-SCA BB-Package-Install is set to the subscriber assigned package ID.

- Cisco-SCA BB-Real-time-monitor-Install is set to real monitor activation value.
- Cisco-SCA BB-Vlink-Upstream-Install is set to the upstream vlink assigned ID.
- Cisco-SCA BB-Vlink-Downstream-Install is set to the downstream vlink assigned ID.

Sample Message:

```
Version        = 1
Message Length = XXX
Command Flags  = PXY
Command Code   = Credit-Control-Answer (272)
Application Id = 16777238
AVPs
    Session-Id         = "27; 3232262425; 1311857000"
    Auth-Application-Id= 16777238
    Origin-Host        = "PCRF host"
    Origin-Realm       = "PCRF Realm"
    CC-Request-Type    = UPDATE_REQUEST (1)
    CC-Request-Number  = 1
    Result-Code        = DIAMETER_SUCCESS
    Cisco-SCA BB-Package-Install = 5
    Cisco-SCA BB-Real-time-monitor-Install = 1
```

The format of the Session-Id is `“pid; ip; time”`, where:

- PID is a 32-bit integer type indicating the unique PID for a specific Gx session.
- IP is a 32-bit unsigned integer type indicating the framed IP of the subscriber for which the session is created. IP is in decimal format.
- TIME is a 32-bit unsigned integer type indicating the time when session is created. Time is in number of seconds starting from January 1, 1970.

Error Handling

No errors are supported.

For a Terminate message if timeout or error occurs, the SCE updates the appropriate counter and closes the session.

Re-Authorize Request (RAR)

Command-Code Field	Command Flags Field	Direction	Description
258	'R' bit set	PCRF to SCE	Sent to provision SCE rules using the PUSH procedure to initiate the provisioning of unsolicited SCE rules. It is used to provision SCE rules for the subscriber.

Message Format:

```
<RA-Request> ::= < Diameter Header: 258, REQ, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Destination-Host }
                 { Re-Auth-Request-Type }
                 [ Framed-IP-Address ]
                 { Subscription-Id }
                 [ Cisco-SCA BB-Package-Install ]
                 [ Cisco-SCA BB-Real-time-monitor-Install ]
                 [ Cisco-SCA BB-Vlink-Upstream-Install ]
                 [ Cisco-SCA BB-Vlink-Downstream-Install ]
                 [ PS-Information ]
                    [3GPP-GGSN-Address]
                    [3GPP-SGSN-Address]
                   [CG-Address]
                    [3GPP-Charging-Id]
                    [Called-Session-Id]
                    [3GPP-GPRS-QoS-Negotiated-Profile]
                    [3GPP-PDP-Type]
                    [3GPP-SGSN-MCC-MNC]
                    [3GPP-GGSN-MCC-MNC]
                    [3GPP-Charging-Characteristics]
                    [3GPP-RAT-Type]
                    [3GPP-Selection-Mode]
                    [3GPP-NSAPI]
                    [3GPP-MS-Timezone]
                    [3GPP-User-Location-Info]
                 [Acct-Multi-Session-ID]
                 [Acct-Session-ID]
                 [Acct-Session-Time]
                 [Calling-Station-ID]
                 [Class]
                 [CUI]
                 [NAS-Identifier]
                 [NAS-IP-Address]
                 [NAS-Port-Type]
                 [User-Name]
                 [3GPP-GGSN-Address-Code-7]
                 [3GPP-IMEISV]
                 [3GPP-IMSI]
                 [3GPP-CG-Address]
                 [3GPP-SGSN-Address-Code-6]
                 [WiMax-Active-Time]
                 [WiMax-BSID]
```

Message Response:

- Session-Id is set to the CCR Session-Id.
- Auth-Application-Id is set to the same value as the CCR.
- Origin-Host is set to the message generating host (PCRF which responds).
- Origin-Realm is set to the PCRF realm.
- CC-Request-Type and CC-Request-Number are set to the same type as in the CCR.
- Subscription-id is set to the subscriber-ID used by the SCE.
- Cisco-SCA BB-Package-Install is set to the subscriber assigned package ID.

- Cisco-SCA BB-Real-time-monitor-Install is set to real monitor activation value.
- Cisco-SCA BB-Vlink-Upstream-Install is set to the upstream vlink assigned ID.
- Cisco-SCA BB-Vlink-Downstream-Install is set to the downstream vlink assigned ID.

Sample Message:

```
Version        = 1
Message Length = XXX
Command Flags  = REQ, PXY
Command Code   = Re-Auth-Request (258)
Application Id = 16777238
AVPs
    Session-Id            = "27; 3232262425; 1311857000"
    Auth-Application-Id   = 16777238
    Origin-Host           = "PCRF Host"
    Origin-Realm          = "PCRF Realm"
    Destination-Realm     = "SCE Realm"
    Destination-Host      = "SCE Host"
    Re-Auth-Request-Type  = AUTHORIZE_ONLY (0)
    Framed-IP-Address     = 10.1.1.1
    Subsscription-Id      = 05412321312
    Cisco-SCA BB-Package-Install = 5
```

The format of the Session-Id is `“pid; ip; time”`, where:

- PID is a 32-bit integer type indicating the unique PID for a specific Gx session.
- IP is a 32-bit unsigned integer type indicating the framed IP of the subscriber for which the session is created. IP is in decimal format.
- TIME is a 32-bit unsigned integer type indicating the time when session is created. Time is in number of seconds starting from January 1, 1970.

Re-Authorize Answer (RAA)

Command-Code Field	Command Flags Field	Direction	Description
258	'R' bit cleared	SCE to PCRF	Sent in response to the RAR command.

Message Format:

```
<RA-Answer> ::=  < Diameter Header: 258, PXY >
                < Session-Id >
                { Origin-Host }
                { Origin-Realm }
                [ Result-Code ]
                [ Error-Message ]
```

Sample Message:

```
Version        = 1
Message Length = XXX
Command Flags  = REQ, PXY
Command Code   = Re-Auth-Request (258)
Application Id = 16777238
AVPs
    Session-Id        = "27; 3232262425; 1311857000"
```

```
Auth-Application-Id= 16777238
Origin-Host        = "SCE Host"
Origin-Realm       = "SCE Realm"
Error-Code         = DIAMETER_SUCCESS
```

The format of the Session-Id is `"pid; ip; time"`, where:

- PID is a 32-bit integer type indicating the unique PID for a specific Gx session.
- IP is a 32-bit unsigned integer type indicating the framed IP of the subscriber for which the session is created. IP is in decimal format.
- TIME is a 32-bit unsigned integer type indicating the time when session is created. Time is in number of seconds starting from January 1, 1970.

Error Handling:

- DIAMETER_UNKNOWN_SESSION_ID is returned if no such session id exits in the SCE database.
- DIAMETER_UNABLE_TO_COMPLY is returned when the RAR is received in the middle of initiating new session (CCR-I was sent). SCE can also return this error code when the update fails for an unknown reason.
- DIAMETER_INVALID_AVP_VALUE is returned when the value of an AVP is not valid; for example, package out of range.
- DIAMETER_MISSING_AVP_SCE is returned when the message format of the RAR is not valid.

Abort Session Request (ASR)

Command-Code Field	Command Flags Field	Direction	Description
274	'R' bit set	Server to access device	May be sent by any server to the access device providing session service, requesting it to stop the session identified by the Session-Id.

Message Format:

```
<ASR> ::=  < Diameter Header: 274, REQ, PXY >
               < Session-Id >
               { Origin-Host }
               { Origin-Realm }
               { Destination-Realm }
               { Destination-Host }
               { Auth-Application-Id }
```

Message Response:

- Origin-Host is set to the SCE host ID (its IP).
- Origin-Realm is set to the SCE-defined realm.
- Destination-Host and Destination-Realm define the PCRF destination. The destination host is not mandatory, it depends on the SCE and PCRF configurations.
- Auth-Application-Id is set to the application ID of the Gx protocol.

Sample Message:

```
Version        = 1
Message Length = XXX
Command Flags  = REQ, PXY
Command Code   = Re-Auth-Request (274)
Application Id = 16777238
AVPs
   Session-Id          = "27; 3232262425; 1311857000"
   Auth-Application-Id= 16777238
   Origin-Host         = "PCRF Host"
   Origin-Realm        = "PCRF Realm"
   Destination-Realm   = "att.com"
   Destination-Host    = "SCE host"
   Auth=Application-id = 16777238
```

The format of the Session-Id is `"pid; ip; time"`, where:

- PID is a 32-bit integer type indicating the unique PID for a specific Gx session.
- IP is a 32-bit unsigned integer type indicating the framed IP of the subscriber for which the session is created. IP is in decimal format.
- TIME is a 32-bit unsigned integer type indicating the time when session is created. Time is in number of seconds starting from January 1, 1970.

Abort Session Answer (ASA)

Command-Code Field	Command Flags Field	Direction	Description
274	'R' bit clear	Access device to server	Sent in response to the ASR. The Result-Code AVP *must* be present; it indicates the disposition of the request.

Message Format:

```
<ASA> ::=  < Diameter Header: 274, PXY >
               < Session-Id >
               { Result-Code }
               { Origin-Host }
               { Origin-Realm }
               [ Error-Message]
```

Message Response:

- Origin-Host is set to the SCE host ID (its IP).
- Origin-Realm is set to the SCE realm.
- Error-Message is set to error description if the SCE is unable to comply.
- The Result-Code is set as follows:
  - If the session identified by Session-Id in the ASR was successfully terminated, Result-Code is set to DIAMETER_SUCCESS.
  - If the session is not currently active, Result-Code is set to DIAMETER_UNKNOWN_SESSION_ID.

  - If the access device does not stop the session for any other reason, Result-Code is set to DIAMETER_UNABLE_TO_COMPLY.

- The SCE tries to comply only in Pull mode.

Sample Message:

```
Version        = 1
Message Length = XXX
Command Flags  = REQ, PXY
Command Code   = Re-Auth-Request (274)
Application Id = 16777238
AVPs
    Session-Id     = "27; 3232262425; 1311857000"
    Result-Code    = DIAMETER_SUCCESS
    Origin-Host    = "SCE Host"
    Origin-Realm   = "SCE Realm"
```

The format of the Session-Id is `"pid; ip; time"`, where:

- PID is a 32-bit integer type indicating the unique PID for a specific Gx session.
- IP is a 32-bit unsigned integer type indicating the framed IP of the subscriber for which the session is created. IP is in decimal format.
- TIME is a 32-bit unsigned integer type indicating the time when session is created. Time is in number of seconds starting from January 1, 1970.

Error Handling:

- DIAMETER_UNKNOWN_SESSION_ID is returned if no such session id exits in the SCE database.
- DIAMETER_UNABLE_TO_COMPLY is returned when ASR is received in the middle of ending a session (CCR-T was sent). It is also returned when the SCE fails to logout the subscriber for an unknown reason.

Gy-Supported Messages

The following messages are supported on the Gy interface:

Supported Gx RLS9 Messages and AVPs—Used between the SCE and the OCS to request credit authorization for a given service.

Credit Control Request (CCR)—The CCR message indicates diameter session create, update, and close.

Credit Control Answer (CCA)—Used between the credit-control server and the SCE to acknowledge a Credit-Control-Request command. The SCE listens to the CCA messages and updates the SCA BB with quota grants, failure conditions, and result codes. The CCA message is also used for failure indication and failure handling.

Re-Authorize Request (RAR)—Sent by any server to the access device that is providing session service, to request that the user be reauthenticated or be reauthorized. In the SCE Gy implementation, RAR messages are used by the OCS to request usage information on either a specific bucket-id or all buckets. The SCE listens to RAR messages and signals SCA BB to send usage information to the OCS. RAR messages arrive in an asynchronous manner from the server and with no correlation to any request completed by the SCE.

Re-Authorize Answer (RAA)—Sent in response to the RAR message. The Result-Code AVP must be present and indicate the disposition of the request. A successful RAA message must be followed by an application-specific authentication and/or authorization message. This message is sent by the Gy application in response to RAR right after the SCA BB is notified that a RAR message has been received.

Credit Control Request (CCR)

Command-Code Field	Command Flags Field	Direction	Description
272	'R' bit set	SCE to OCS	Sent to request credit authorization for a given service.

The Auth-Application-Id value is set to 4, indicating the Diameter credit-control application.

Table A-1 lists the CCR message structure.

Table A-1 CCR Message Structure

AVP Name	Category	AVP Code (Code / Vendor-id)	Value	Comment
Session-Id	M[1]	263	String Format: <pid; ip; time>	Session-Id.
Origin-Host	M	264	DiameterIdentifier	IP of the SCE platform.
Origin-Realm	M	296	DiameterIdentifier	Configured value.
Destination-Realm	M	283	DiameterIdentifier	Configured value in CCR (Initial). For subsequent CCRs, the Origin-Realm received in the last CCA is used as Destination-Realm.

Table A-1 CCR Message Structure (continued)

AVP Name	Category	AVP Code (Code / Vendor-id)	Value	Comment
Destination-Host	Oc[2]	293	DiameterIdentifier	Not sent in the first CCR message. The Origin-Host in the CCA is used as Destination-Host in the next CCR message.
Auth-Application-Id	M	258	4	Value for DCCA.
Service-Context-Identifier	M	461	—	—
CC-Request-Type	M	416	1 = INITIAL_REQUEST 2 = UPDATE_REQUEST 3 = TERMINATION_ REQUEST 4 = EVENT_REQUEST	Type “EVENT_REQUEST” is not supported.
CC-Request-Number	M	415	A monotonically increasing number	Value of “0” is used for CCR (INITIAL_REQUEST).
Event-Timestamp	Oc	55	Time when quota is requested	—
Subscription-Id	Om[3]	443	Grouped AVP	Grouped AVP consisting of Subscription-Id-Type and Subscription-Id-Data.
Subscription-Id-Type	Om	450	END_USER_E164 (0)	—
Subscription-Id-Data	Om	444	MSISDN (string)	—
Termination-Cause	Oc	295	Integer value (as per RFC 3588)	Only sent in CCR (FINAL)
Multiple-Services-Indicator	Om	455	MULTIPLE_SERVICES_ SUPPORTED (1)	Present only in CCR (INITIAL)
Multiple-Services-Credit-Control (see separate description for Multiple Services Credit Control AVP)	Om	456	Grouped AVP	See Multiple Services Credit Control AVP. Multiple of these attributes can be present. Contains the usage for each category.
Service-Information AVP	Om	—	Grouped AVP	—
PS-Information	Om	—	Grouped AVP	—
Called-Station-Id	Oc	30	APN name (string)	In PS-Information.
SGSN-Address	Oc	1228	IPv4 Address	Subscriber attributes.

Table A-1 CCR Message Structure (continued)

AVP Name	Category	AVP Code (Code / Vendor-id)	Value	Comment
3GPP-GPRS-QoS-Negotiated-profile	Oc	5/10415	Negotiated QoS profile	QoS profile of the Primary PDP context will be sent. However, if a primary PDP is deleted before the secondary PDPs, subsequent CCR messages contain the negotiated QoS of the first Secondary PDP context. (Subscriber attributes, received from Gx or SCE subscriber API) (in PS-Information).
3GPP-SGSN-MCC-MNC	Oc	18/10415	—	Subscriber attributes, received from Gx or SCE subscriber API (in PS-Information).
3GPP-Charging-Characteristics	Oc	13/10415	Charging Char received from SGSN	—

1. This parameter is mandatory and must be present in the event/CDR.
2. This is a parameter that, if provisioned by the operator to be present, is included in the events/CDRs when the specified conditions are met. In other words, an Oc parameter that is configured to be present is a conditional parameter.
3. This is a parameter that, if provisioned by the operator to be present, is included in the events/CDRs. In other words, an Om parameter that is provisioned to be present is a mandatory parameter.

CCR Message Formats

This section contains:

CCR Initial Message Fields

```
<Credit-Control-Request> ::= < Session-Id >
                              { Origin-Host }
                              { Origin-Realm }
                              { Destination-Realm }
                              { Auth-Application-Id }
                              { Service-Context-Id }
                              { CC-Request-Type }
                              { CC-Request-Number }
                              [ Event-Timestamp ]
                             *[ Subscription-Id ]
                                  { Subscription-Id-Type }
                                  { Subscription-Id-Data }
                              [ Multiple-Services-Indicator ]
                             *[ Multiple-Services-Credit-Control ]
                                  [ Requested-Service-Unit ]
                                 *[ Service-Identifier ]
                                  [ Rating-Group ]
                                  [ Service-Information ]
                                    [ PS-Information ]
                                       [3GPP-GGSN-Address]
                                       [3GPP-SGSN-Address]
                                       [3GPP-Charging-Id]
                                       [Called-Session-Id]
                                       [3GPP-GPRS-QoS-Negotiated-Profile]
                                       [3GPP-PDP-Type]
                                       [3GPP-SGSN-MCC-MNC]
                                       [3GPP-GGSN-MCC-MNC]
                                       [3GPP-Charging-Characteristics]
                                       [3GPP-RAT-Type]
                                       [3GPP-Selection-Mode]
                                       [3GPP-NSAPI]
                                       [3GPP-MS-Timezone]
                                       [3GPP-User-Location-Info]
                              [Acct-Multi-Session-ID]
                              [Acct-Session-ID]
                              [Acct-Session-Time]
                              [Calling-Station-ID]
                              [Class]
                              [CUI]
                              [Framed-IP-Address]
                              [NAS-Identifier]
                              [NAS-IP-Address]
                              [NAS-Port-Type]
                              [User-Name]
                              [3GPP-GGSN-Address-Code-7]
                              [3GPP-IMEISV]
                              [3GPP-IMSI]
                              [3GPP-CG-Address]
                              [3GPP-SGSN-Address-Code-6]
                              [WiMax-Active-Time]
                              [WiMax-BSID]
```

CCR Update Message Fields

```
<Credit-Control-Request> ::= < Session-Id >
                              { Origin-Host }
                              { Origin-Realm }
                              { Destination-Realm }
                              { Auth-Application-Id }
                              { Service-Context-Id }
                              { CC-Request-Type }
                              { CC-Request-Number }
                              [ Destination-Host ]
                              [ Event-Timestamp ]
                             *[ Subscription-Id ]
                                  { Subscription-Id-Type }
                                  { Subscription-Id-Data }
                             *[ Multiple-Services-Credit-Control ]
                                 *[ Used-Service-Unit ]
                                      [ Tariff-Change-Usage ]
                                      [ CC-Time ]
                                      [ CC-Total-Octets ]
                                      [ CC-Service-Specific-Units ]
                                      [ Reporting-Reason ]
                                      [ CC-Input-Octets ]
                                      [ CC-Output-Octets ]
                                 *[ Service-Identifier ]
                                  [ Rating-Group ]
                              [ Service-Information ]
                                [PS-Information ]
                                    [3GPP-GGSN-Address]
                                    [3GPP-SGSN-Address]
                                    [3GPP-Charging-Id]
                                    [Called-Session-Id]
                                    [3GPP-GPRS-QoS-Negotiated-Profile]
                                    [3GPP-PDP-Type]
                                    [3GPP-SGSN-MCC-MNC]
                                    [3GPP-GGSN-MCC-MNC]
                                    [3GPP-Charging-Characteristics]
                                    [3GPP-RAT-Type]
                                    [3GPP-Selection-Mode]
                                    [3GPP-NSAPI]
                                    [3GPP-MS-Timezone]
                                    [3GPP-User-Location-Info]
                              [Acct-Multi-Session-ID]
                              [Acct-Session-ID]
                              [Acct-Session-Time]
                              [Calling-Station-ID]
                              [Class]
                              [CUI]
                              [Framed-IP-Address]
                              [NAS-Identifier]
                              [NAS-IP-Address]
                              [NAS-Port-Type]
                              [User-Name]
                              [3GPP-GGSN-Address-Code-7]
                              [3GPP-IMEISV]
                              [3GPP-IMSI]
                              [3GPP-CG-Address]
                              [3GPP-SGSN-Address-Code-6]
                              [WiMax-Active-Time]
                              [WiMax-BSID]
```

CCR Final Message Fields

```
<Credit-Control-Request> ::= < Session-Id >
                              { Origin-Host }
                              { Origin-Realm }
                              { Destination-Realm }
                              { Auth-Application-Id }
                              { Service-Context-Id }
                              { CC-Request-Type }
                              { CC-Request-Number }
                              [ Destination-Host ]
                              [ Event-Timestamp ]
                             *[ Subscription-Id ]
                                  { Subscription-Id-Type }
                                  { Subscription-Id-Data }
                              [ Termination-Cause ]
                             *[ Multiple-Services-Credit-Control ]
                                 *[ Used-Service-Unit ]
                                      [ Tariff-Change-Usage ]
                                      [ CC-Time ]
                                      [ CC-Total-Octets ]
                                      [ CC-Service-Specific-Units ]
                                      [ Reporting-Reason ]
                                      [ CC-Input-Octets ]
                                      [ CC-Output-Octets ]
                                 *[ Service-Identifier ]
                                  [ Rating-Group ]
```

Credit Control Answer (CCA)

Command-Code Field	Command Flags Field	Direction	Description
272	'R' bit cleared	Credit control server to SCE.	Sent to acknowledge a CCR command.

The SCE listens to CCA messages and updates SCA BB with grant quotas, failure conditions, and result codes. CCA is also used for failure indication and failure handling.

Table A-2 lists the CCA message structure.

Table A-2 CCA Message Structure

AVP name	Category	AVP Code (Code / Vendor-Id)	Value	Comment
Session-Id	M[1]	263	String	
Origin-Host	M	264	DiameterIdentifier	Address of the DCCA server.
Origin-Realm	M	296	DiameterIdentifier	Realm of the DCCA server.
Result-Code	M	268	Integer value (as per RFC 3588 & DCCA draft)	—
Auth-Application-Id	M	258	4	Value for DCCA.

Table A-2 CCA Message Structure (continued)

AVP name	Category	AVP Code (Code / Vendor-Id)	Value	Comment
CC-Request-Type	M	416	1 = INITIAL_REQUEST 2 = UPDATE_REQUEST 3 = TERMINATION_ REQUEST 4 = EVENT_REQUEST	Value 4 (Event) is not supported.
CC-Request-Number	M	415	Same as the one sent in corresponding CCR message	—
CC-Session-Failover	Oc[2]	—	—	—
Multiple-Services-Credit-Control	Om[3]	456	Grouped AVP	Contains the quota granted. There can be multiple instances of this attribute, one for each category.
Service-Context-Id	Oc	—	—	—
Subscription-Id	Oc	—	—	—
CC-Failure-Handling	Oc	—	—	—
Failed-AVP	Oc	279	Grouped AVP. Contains the list of attributes causing failure condition	Optionally present. If the Result-Code is not SUCCESS. There can be multiple instances of this AVP.

[1] This parameter is mandatory and must be present in the event/CDR.

[2] This is a parameter that, if provisioned by the operator to be present, is included in the events/CDRs when the specified conditions are met. In other words, an Oc parameter that is configured to be present is a conditional parameter.

[3] This is a parameter that, if provisioned by the operator to be present, is included in the events/CDRs. In other words, an Om parameter that is provisioned to be present is a mandatory parameter.

CCA Message Format

```
<Credit-Control-Answer> ::=   < Session-Id >
                              { Result-Code }
                              { Origin-Host }
                              { Origin-Realm }
                              { Auth-Application-Id }
                              { CC-Request-Type }
                              { CC-Request-Number }
                              [ CC-Session-Failover ]
                             *[ Multiple-Services-Credit-Control ]
                                  [ Granted-Service-Unit ]
                                      [ Tariff-Time-Change ]
                                      [ CC-Time ]
                                      [ CC-Total-Octets ]
                                      [ CC-Input-Octets ]
                                      [ CC-Output-Octets ]
                                      [ CC-Service-Specific-Units ]
                                 *[ Service-Identifier ]
                                  [ Rating-Group ]
                                  [ Validity-Time ]
                                  [ Result-Code ]
                                  [ Final-Unit-Indication ]
                                      { Final-Unit-Action }
                                  [ Time-Quota-Threshold ]
                                  [ Volume-Quota-Threshold ]
                                  [ Unit-Quota-Threshold ]
                                  [ Quota-Holding-Time ]
                                  [ Quota-Consuption-Time ]
                              [ Service-Context-Id ]
                             *[ Subscription-Id ]
                                  { Subscription-Id-Type }
                                  { Subscription-Id-Data }
                              [ Credit-Control-Failure-Handling ]
                              [ CC-Session-Failover ]
                             *[ Failed-AVP ]
```

Re-Auth Request (RAR)

Command-Code Field	Command Flags Field	Direction	Description
258	'R' bit set	Server to access device	Sent to the access device that is providing session service to request that the user be reauthenticated or reauthorized.

In the SCE, Gy implementation of RAR messages may be used by the OCS to request usage information about a specific bucket-id or about all the buckets. The SCE listens to the RAR messages and signals the SCA BB to send usage information to the OCS.

RAR messages may arrive asynchronously from the server, with no correlation to any request from the SCE. The SCE behavior upon receiving an RAR message is common to other scenarios as well, such as logout or package change.

Table A-3 lists the RAR message structure.

Table A-3 RAR Message Structure

AVP Name	Category	AVP Code (Code/Vendor Id)	Value	Comment
Session-Id	M[1]	263	String	—
Origin-Host	M	264	Host name of Diameter server	—
Origin-Realm	M	296	Origin realm of Diameter server	—
Destination-Realm	M	283	Destination realm of diameter peer	—
Destination-Host	M	293	Host name of diameter peer	—
Auth-Application-Id	M	258	4	—
Re-Auth-Request-Type	M	285	Authorize-Only	—
Rating-Group	Oc[2]	432	Category Id	Presence of this AVP means that reauthorization is done for this specific category.

[1] This parameter is mandatory and must be present in the event/CDR.

[2] This is a parameter that, if provisioned by the operator to be present, is included in the events/CDRs when the specified conditions are met. In other words, an Oc parameter that is configured to be present is a conditional parameter.

RAR Message Format

```
<Re-Auth-Request> ::= < Session-Id >
                      { Origin-Host }
                      { Origin-Realm }
                      { Destination-Realm }
                      { Destination-Host }
                      { Auth-Application-Id }
                      { Re-Auth-Request-Type }
                      [ Rating-Group ]
```

Re-Auth Answer (RAA)

Command-Code Field	Command Flags Field	Direction	Description
258	'R' bit cleared	Access device to server	Sent in response to the RAR.

The Result-Code AVP *must* be present, and indicates the disposition of the request.

A successful RAA message *must* be followed by an application-specific authentication, authorization message, or both.

This message is sent by the Gy application in response to RAR right after the SCA BB is notified with the RAR.

Table A-4 lists the RAA message structure.

Table A-4 RAA Message Structure

AVP Name	Category	AVP Code (Code/Vendor Id)	Value	Comment
Session-Id	M[1]	263	String Format: <pid; ip; time>	—
Result-Code	M	268	2001, 2002	A value of 2001 is sent if no CCR (Update) is sent. A value of 2002 is sent if a subsequent CCR (Update) follows.
Origin-realm	M	296	DiameterIdentifier	Configured value.
Origin-Host	M	264	DiameterIdentifier	Configured value.

[1] This parameter is mandatory and must be present in the event/CDR.

RAA Message Format

```
<Re-Auth-Answer> ::= < Session-Id >
                     { Origin-Host }
                     { Origin-Realm }
              { Result-Code }
```

Supported Gy Messages and AVPs

Table A-5 lists the Gy messages and the AVPs used for Gy client interface support.

Table A-5 Supported Gy Messages and AVPs

Messages						Gy Message Fields	Category	Comment
CCR Initial	CCR Update	CCR Termination	CCA	RAR	RAA	–	—	—
+	+	+	+	+	+	Session-Id	M[1]	—
—	—	—	+	—	+	Result-Code	M	—
+	+	+	+	+	+	Origin-Host	M	—
+	+	+	+	+	+	Origin-Realm	M	—
+	+	+	—	+	—	Destination-Realm	M	—
+	+	+	+	+	—	Auth-Application-Id	M	—
—	—	—	—	+	—	Re-Auth-Request-Type	M	—
+	+	+	—	—	—	Service-Context-Identifier	M	—
+	+	+	+	—	—	CC-Request-Type	M	—
+	+	+	+	—	—	CC-Request-Number	M	—

Table A-5 Supported Gy Messages and AVPs (continued)

Messages						Gy Message Fields	Category	Comment
CCR Initial	CCR Update	CCR Termination	CCA	RAR	RAA	–	—	—
—	—	—	+	—	—	CC-Session-Failover	Oc[2]	—
—	—	—	—	+	—	Destination-Host	Oc (M for RAR)	—
—	—	—	—	(+)	—	Rating-Group	Oc	—
+	+	+	—	—	—	Event-Timestamp	Om[3]	—
+	+	+	—	—	—	Subscription-Id	Om	Grouped AVP
+	+	+	—	—	—	Subscription-Id-Type	Om	—
+	+	+	—	—	—	Subscription-Id-Data	Oc	—
—	—	+	—	—	—	Termination-Cause	Om	Reporting reason is used for regular logout, unsupported tariff-change, and unsupported unit type.
+	—	—	—	—	—	Multiple-Services-Indicator	Om	—
+	+	+	+	—	—	Multiple-Services-Credit-Control	Om	Grouped AVP
+	+	+	—	—	—	Service-Identifier	—	—
+	—	—	—	—	—	Requested-Service-Unit	Oc	Empty
—	+	+	—	—	—	Used-Service-Unit	Oc	Grouped AVP
—	+	+	—	—	—	Reporting-Reason	Oc	—
—	+	+	—	—	—	Tariff-Change-Usage	Oc	—
—	+	+	—	—	—	CC-Time	Oc	—
—	+	+	—	—	—	CC-Total-Octets	Oc	—
—	+	+	—	—	—	CC-Input-Octets	Oc	—
—	+	+	—	—	—	CC-Output-Octets	Oc	—
—	+	+	—	—	—	CC-Service-Specific-Units	Oc	—
—	—	—	+	—	—	Granted-Service-Unit	Oc	Grouped AVP
—	—	—	+	—	—	Tariff-Time-Change	Oc	—
—	—	—	+	—	—	CC-Time	Oc	—
—	—	—	+	—	—	CC-Total-Octets	Oc	—
—	—	—	+	—	—	CC-Input-Octets	Oc	—
—	—	—	+	—	—	CC-Output-Octets	Oc	—

Table A-5 Supported Gy Messages and AVPs (continued)

Messages						Gy Message Fields	Category	Comment
CCR Initial	CCR Update	CCR Termination	CCA	RAR	RAA	–	—	—
—	—	—	+	—	—	CC-Service-Specific-Units	Oc	—
(+)	+	+	+	—	—	Rating-Group	Oc	—
—	—	—	+	—	—	Validity-Time	Oc	—
—	—	—	+	—	—	Result-Code	Oc	Considered only if the Result-Code value present at the command level is SUCCESS. The value is defined by 3GPP TS 32.299 V6.6.0 section 7.15.
—	—	—	+	—	—	Final-Unit-Indication	Oc	Grouped AVP
—	—	—	+	—	—	Final-Unit-Action	Oc	TERMINATE, REDIRECT, or RESTRICT_ACCESS
—	—	—	+	—	—	Time-Quota-Threshold	Oc	—
—	—	—	+	—	—	Volume-Quota-Threshold	Oc	—
—	—	—	+	—	—	Unit-Quota-Threshold	Oc	—
—	—	—	+	—	—	Quota-Holding-Time	Oc	—
—	—	—	+	—	—	Quota-Consumption-Time	Oc	—
—	—	—	+	—	—	Credit-Control-Failure-Handling	—	—
+	—	—	—	—	—	Service-Information AVP	Om	Grouped AVP
+	—	—	—	—	—	PS-Information	Om	Grouped AVP
+	—	—	—	—	—	Called-Station-Id	Om	—
+	—	—	—	—	—	SGSN-Address	Om	—
+	—	—	—	—	—	3GPP-GPRS-Negotiated-QOS-Profile	Om	—
+	—	—	—	—	—	3GPP-SGSN-MCC-MNC	Om	—
+	—	—	—	—	—	3GPP-Charging-Characteristics	Om	—

1. This parameter is mandatory and must be present in the event/CDR.
2. This is a parameter that, if provisioned by the operator to be present, is included in the events/CDRs when the specified conditions are met. In other words, an Oc parameter that is configured to be present is a conditional parameter.
3. This is a parameter that, if provisioned by the operator to be present, is included in the events/CDRs. In other words, an Om parameter that is provisioned to be present is a mandatory parameter.

Multiple Services Credit Control AVP

The Multiple Services Credit Control (MSCC) AVP is used for granting and reporting quota for each bucket (rating-group). Figure A-2 illustrates the structure of this attribute, and Table A-6 lists the structure.

When the MSCC AVP is present in CCA messages, it represents quota being granted. When it is present in CCR messages, it represents usage being reported. If quota/usage is being reported for more than one rating-group, then multiple MSCC AVPs are present in the message.

There are some attributes that can be present at the command level and the MSCC level.

- Result-Code

  If the Result-Code present at the command level is SUCCESS, the Result-Code present at MSCC level takes effect.

- Validity-Time

  The Validity-Time present at the command level applies to all the categories. If Validity-Time is present at MSCC level, its value is used for that particular category.

- Requested-Service-Unit

  This AVP must be present at the command level for CCR (initial). When the quota request for a particular category is made using CCR (update), it is present at the MSCC level for that category.

Figure A-2 MSCC AVP Structure

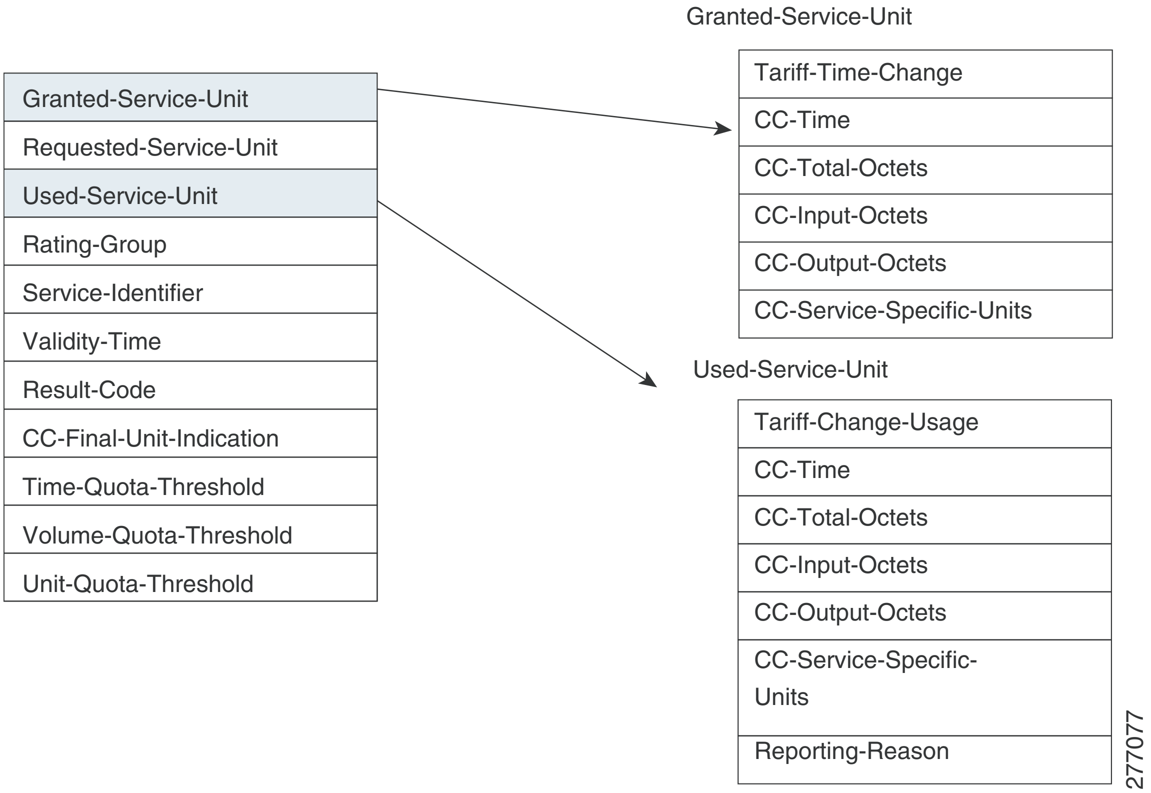


Table A-6 MSCC AVP Structure

AVP Name	Category	AVP Code (Code / Vendor-Id)	Value	Comment
Granted-Service-Unit	Oc[1]	431	Grouped AVP	Present inside MSCC of a CCA (initial) and CCA (update) message.
Requested-Service-Unit	Oc	437	Empty value	Conditionally present inside MSCC of a CCR (update) message.
Used-Service-Unit	Oc	446	Grouped AVP	Present inside MSCC of a CCR (update) and CCR (final) message. There can be multiple instances of this AVP.
Rating-Group	Oc	432	—	Used to indicate service.
Validity-Time	Oc	448	Time until quota is valid	A value of “0” is considered invalid. Present inside MSCC of CCA messages.
Result-Code	Om[2]	268	Value as per DCCA RFC	Considered only if the Result-Code value present at command level is SUCCESS. Present inside MSCC of CCA messages.
CC-Final-Unit-Indication	Oc	—	Grouped AVP	—
Final Unit Indication	Oc	—	—	—
Time-Quota-Threshold	Oc	868/10415	Quota threshold for time quota in seconds	Present inside MSCC of CCA messages. This AVP is ignored if no time quota is granted (that is, CC-Time AVP is not present inside Granted-Service-Unit AVP).
Volume-Quota-Threshold	Oc	869/10415	Quota threshold for volume quota in octets	Present inside MSCC of CCA messages. This AVP is ignored if no volume quota is granted (that is, CC-Total-Octets is not present inside Granted-Service-Unit AVP).
Unit-Quota-Threshold	Oc	869/10415	Quota threshold for unit quota in octets	Present inside MSCC of CCA messages. This AVP is ignored if no unit quota is granted (i.e. CC-Unit-Quota is not present inside Granted-Service-Unit AVP).

Table A-6 MSCC AVP Structure (continued)

AVP Name	Category	AVP Code (Code / Vendor-Id)	Value	Comment
CC-Time	Oc	420	Time quota in seconds	Present in Granted-Service-Unit AVP and Used-Service-Unit AVP.
CC-Service-Specific-Units	Oc	417	Events quota	Refer to the service identified in the Service-Identifier AVP.
CC-Total-Octets	Oc	421	Volume quota in octets (64 bit number)	Present in Granted-Service-Unit AVP and Used-Service-Unit AVP.
Tariff-Time-Change	Oc	451	Number of seconds since 01/01/1900 UTC	Refer to the time when tariff of the service will be changed. Present in Granted-Service-Unit AVP.
Tariff-Change-Usage	Oc	452	UNIT_BEFORE_TARIFF_CHANGE (0), UNIT_AFTER_TARIFF_CHANGE (1), UNIT_UNDETERMINATE (2)	Present in Used-Service-Unit AVP.
CC-Input-Octets	Oc	412	Number of octets received from the end user	Present in Used-Service-Unit.
CC-Output-Octets	Oc	414	Number of octets sent to the end user	Present in Used-Service-Unit.

[1] This is a parameter that, if provisioned by the operator to be present, is included in the events/CDRs when the specified conditions are met. In other words, an Oc parameter that is configured to be present is a conditional parameter.

[2] This is a parameter that, if provisioned by the operator to be present, is included in the events/CDRs. In other words, an Om parameter that is provisioned to be present is a mandatory parameter.

Gy Support Session and Call Flows

This section provides information on Gy support session initiation, quota usage reporting, package changes, and call flows.

Initiating Session

Once a login event occurs on SCA BB, it sends a Session Creation RDR if the subscriber quota is externally provisioned. The Gy interface listens to these messages and in return sends a CCR initial message to the OCS with or without quota usage information. This process is completed to allow PDP context creation on the OCS as quickly as possible.

Table A-7 lists the required fields in the CCR initial message and their sources and Figure A-3 displays the session creation call flow.

Table A-7 CCR Initial Message Fields and Sources

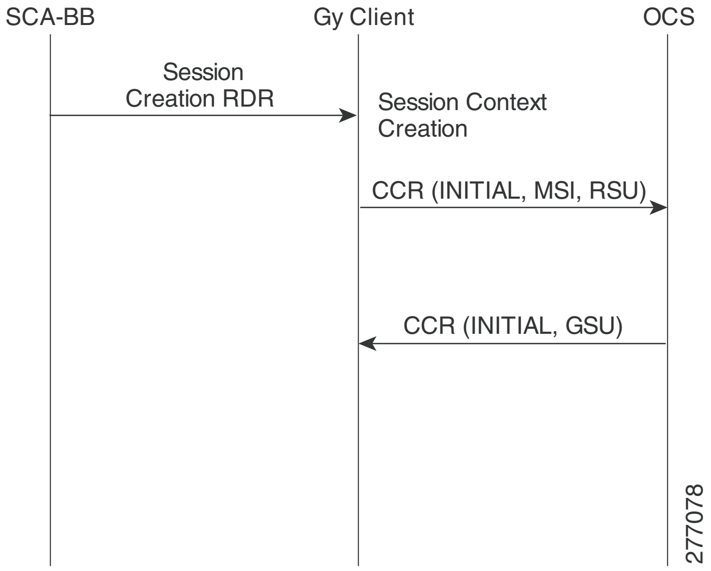
Gy Message Fields	Category		Internal Interface
–	—	**Internal Resource**	**Session Creation RDR**
Session-Id	M[1]	Session ID pool	—
Origin-Host	M	Diameter Config	—
Origin-Realm	M	Diameter Config	—
Destination-Realm	M	Diameter Routing Table	—
Auth-Application-Id	M	Preconfigured	—
Service-Context-Identifier	M	Preconfigured	—
CC-Request-Type	M	—	Reporting-Reason
CC-Request-Number	M	Session context CCR counter	—
Event-Timestamp	Om[2]	System clock	—
Subscription-Id	Om	—	—
Subscription-Id-Type	Om	Preconfigured	—
Subscription-Id-Data	Oc[3]	—	Subscriber id
Multiple-Services-Indicator	Om	Always MULTIPLE_SERVICES_ SUPPORTED (1)	—
Multiple-Services-Credit-Control	Om	—	—
Service-Identifier	—	—	—
Requested-Service-Unit	Oc	—	—
Rating-Group	Oc	—	Bucket-id
Service-Information AVP	Om	—	—
PS-Information	Om	—	—
Called-Station-Id	Om	Subscriber's attributes	—
SGSN-Address	Om	Subscriber's attributes	—

Table A-7 CCR Initial Message Fields and Sources (continued)

Gy Message Fields	Category		Internal Interface
–	—	**Internal Resource**	**Session Creation RDR**
3GPP-GPRS-Negotiated-QOS-Profile	Om	Subscriber’s attributes	—
3GPP-SGSN-MCC-MNC	Om	Subscriber’s attributes	—
3GPP-Charging-Characteristics	Om	Subscriber’s attributes	—

1. This parameter is mandatory and must be present in the event/CDR.
2. This is a parameter that, if provisioned by the operator to be present, is included in the events/CDRs. In other words, an Om parameter that is provisioned to be present is a mandatory parameter.
3. This is a parameter that, if provisioned by the operator to be present, is included in the events/CDRs when the specified conditions are met. In other words, an Oc parameter that is configured to be present is a conditional parameter.

Figure A-3 Session Creation



Reporting Quota Usage

The SCE reports the quota usage for each category under the circumstances listed in Table A-8.

Table A-8 Quota Reporting Usage Conditions and Reasons

Condition	Reporting Reason
Threshold hit	THRESHOLD
Quota breach	QUOTA_EXHAUSTED
Quota Holding Timer expired	QHT
Validity Timer expired	VALIDITY_TIME
Package Change	RATING_CONDITION_CHANGE (TERMINATE and INITIAL)
Server initiated reauthorization procedure	FORCED_REAUTHORIZATION

Quota usage is reported by SCA BB using the Quota Status RDR, the Gy client listens to these messages and delivers them by a CCR update message to the OCS.

Table A-9 lists the structure of a CCR update message and the source for each field and Figure A-4 displays the quota usage update call flow.

Table A-9 CCR Update Message Structure

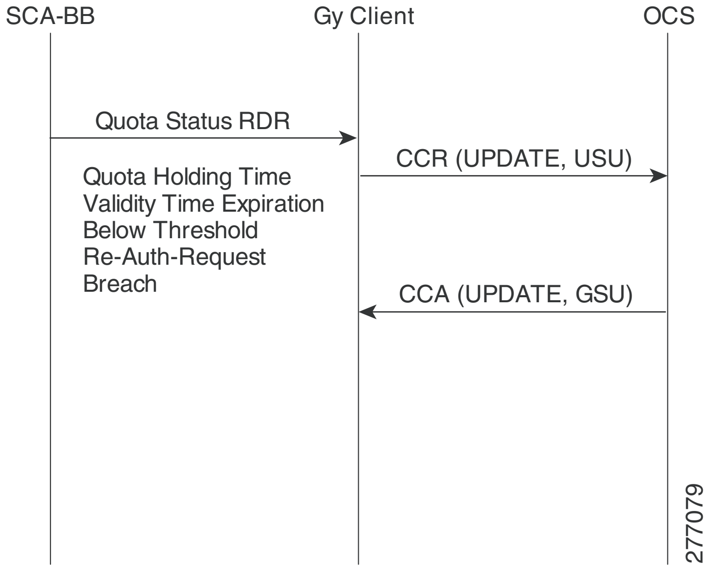
Gy Message Fields	Category	Internal Resource	Internal Interface Quota Status RDR
Session-Id	M[1]	Session ID pool	—
Origin-Host	M	Diameter Config	—
Origin-Realm	M	Diameter Config	—
Destination-Realm	M	Diameter Routing Table	—
Auth-Application-Id	M	Preconfigured	—
Service-Context-Identifier	M	Preconfigured	—
CC-Request-Type	M	—	Reporting-Reason
CC-Request-Number	M	Session context CCR counter	—
Event-Timestamp	Om[2]	System clock	—
Subscription-Id	Om	—	—
Subscription-Id-Type	Om	Preconfigured	—
Subscription-Id-Data	Oc[3]	—	Subscriber id
Multiple-Services-Credit-Control	Om	—	—
Service-Identifier	—	—	—
Rating-Group	Oc	—	Bucket-id
Used-Service-Unit	Oc	—	—
Reporting-Reason	Oc	—	Reporting-Reason
Tariff-Change-Usage	Oc	—	Tarrif-Change-Usage
CC-Time	Oc	—	Units-Type +Unit-Amount
CC-Total-Octets	Oc	—	Units-Type + Unit-Amount
CC-Input-Octets	Oc	—	Units-Type + Unit-Amount
CC-Output-Octets	Oc	—	Units-Type + Unit-Amount
CC-Service-Specific-Units	Oc	—	Units-Type + Unit-Amount

[1] This parameter is mandatory and must be present in the event/CDR.

[2] This is a parameter that, if provisioned by the operator to be present, is included in the events/CDRs. In other words, an Om parameter that is provisioned to be present is a mandatory parameter.

[3] This is a parameter that, if provisioned by the operator to be present, is included in the events/CDRs when the specified conditions are met. In other words, an Oc parameter that is configured to be present is a conditional parameter.

Figure A-4 Quota Usage Update



The exact structure of CCR update is also used for CCR terminate. Figure A-5 displays the session termination initiated by the SCA BB call flow. Figure A-6 displays the reauthorization request initiated by the OCS.

Figure A-5 Session Termination Initiated by SCA BB

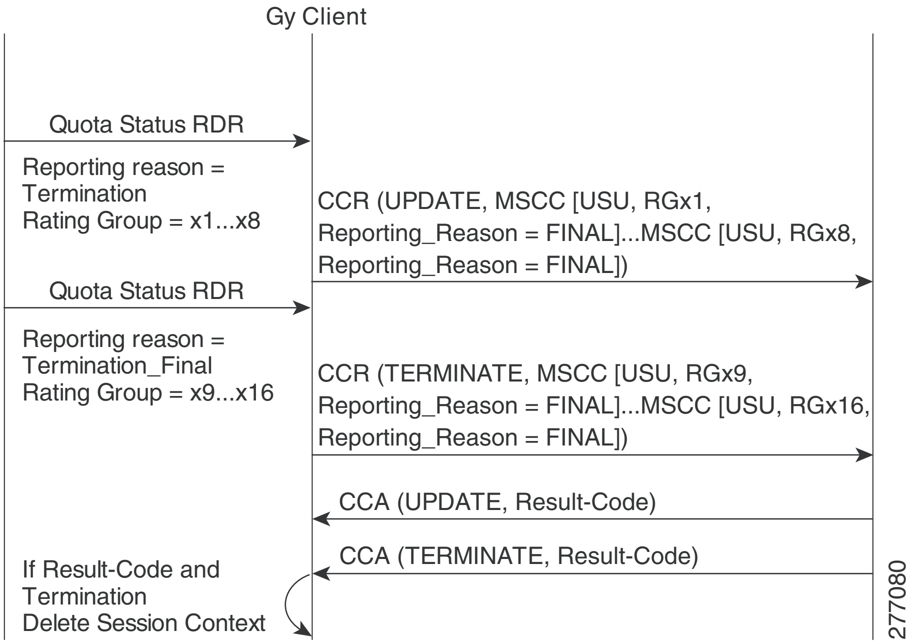
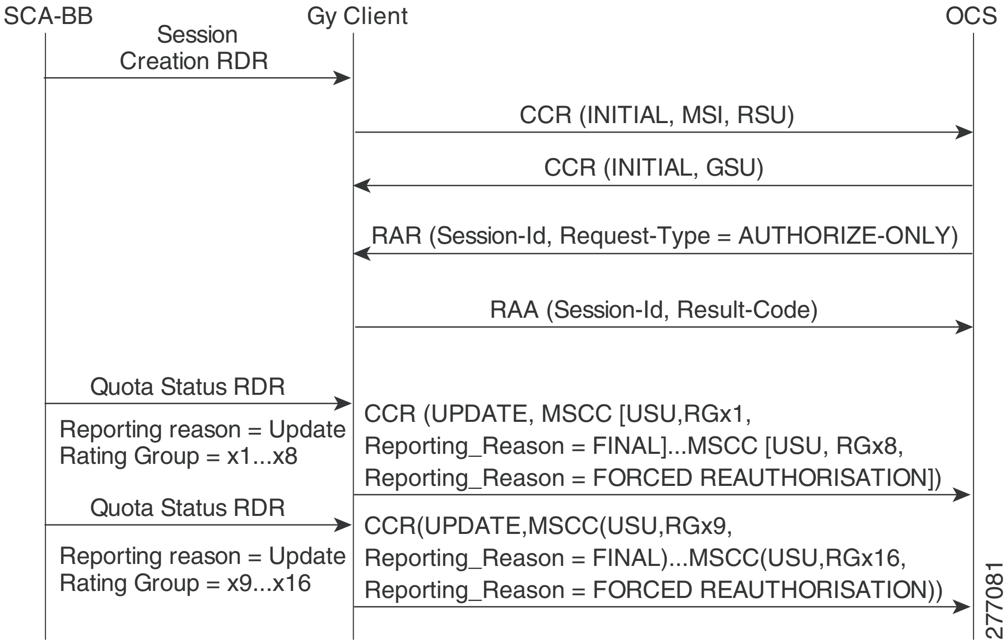

Gy Client
Quota Status RDR
Reporting reason =
Termination
Rating Group = x1...x8
CCR (UPDATE, MSCC [USU, RGx1,
Reporting_Reason = FINAL]...MSCC [USU, RGx8,
Reporting_Reason = FINAL])
Quota Status RDR
Reporting reason =
Termination_Final
Rating Group = x9...x16
CCR (TERMINATE, MSCC [USU, RGx9,
Reporting_Reason = FINAL]...MSCC [USU, RGx16,
Reporting_Reason = FINAL])
CCA (UPDATE, Result-Code)
CCA (TERMINATE, Result-Code)
If Result-Code and
Termination
Delete Session Context
277080

Figure A-6 ***Reauthorization Request Initiated by the OCS***


SCA-BB
Gy Client
OCS
Session Creation RDR
CCR (INITIAL, MSI, RSU)
CCR (INITIAL, GSU)
RAR (Session-Id, Request-Type = AUTHORIZE-ONLY)
RAA (Session-Id, Result-Code)
Quota Status RDR
Reporting reason = Update
Rating Group = x1...x8
CCR (UPDATE, MSCC [USU,RGx1,
Reporting_Reason = FINAL]...MSCC [USU, RGx8,
Reporting_Reason = FORCED REAUTHORISATION])
Quota Status RDR
Reporting reason = Update
Rating Group = x9...x16
CCR(UPDATE,MSCC(USU,RGx9,
Reporting_Reason = FINAL)...MSCC(USU,RGx16,
Reporting_Reason = FORCED REAUTHORISATION))
277081

Package Change

Upon package change, the SCA BB sends a Session Termination RDR, which contains the final indication and usage reporting on all the buckets and the reporting reason of the pre-package. As a result, the Gy interface sends a CCR final message with usage information. After this, the SCA BB sends a Quota Status RDR with reporting reason of postpackage, the Gy client issues a CCR initial message with bucket IDs. Figure A-7 displays the tariff change call flow and Figure A-8 displays the package change call flow.

Figure A-7 Tariff Change

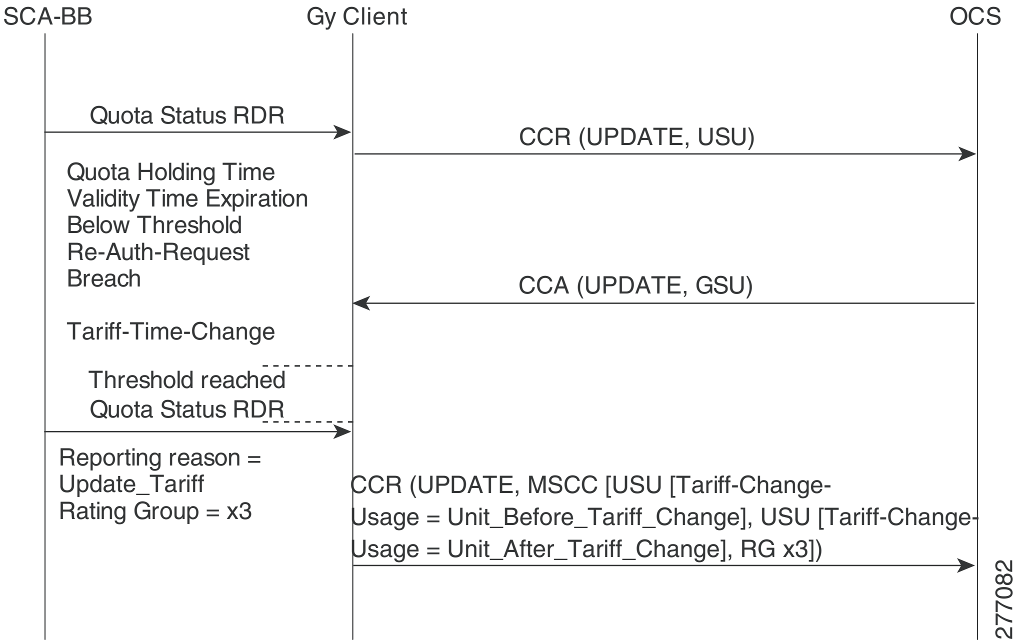
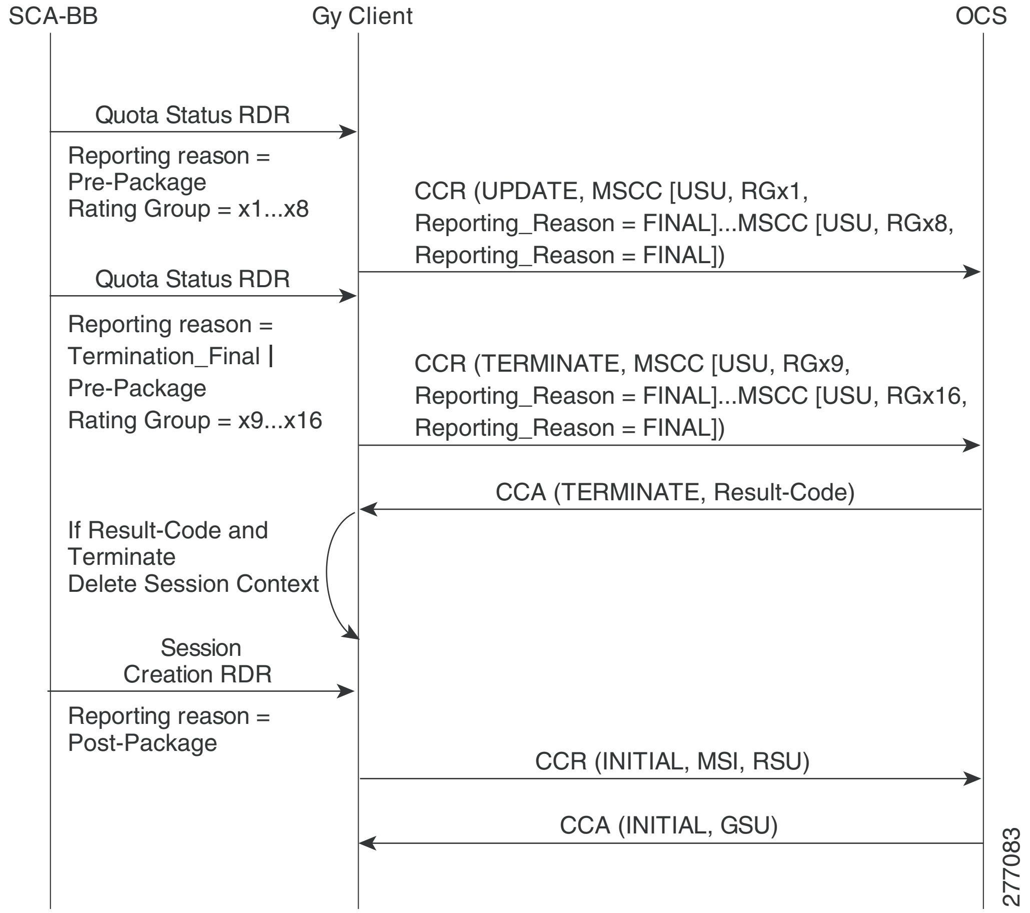


Figure A-8 Package Change



Note The SCE immediately forwards messages from the data plane to OCS without buffering it. It does not wait to receive the CCA message from OCS before sending the next message. Robust OCS implementation should be able to cope with receiving the CCR-U message from the SCE before the CCA-I message was sent and receiving the CCR-T message before the CCA-U message was sent.

supported Gx RLS9 Messages and AVPs

Table A-10 summarizes the message types and AVPs that Gx RLS9 supports.

Table A-10 Supported Gx RLS9 Messages and AVPs

AVP Name	AVP Code (Code / Vendor-Id)	Value Type	Value	Comment
Event-Trigger	1006/ 10415 (3GPP)	Enumerated	USAGE_REPORT (26)—PCRF provides the Usage-Monitoring-Information AVP.	Used in CCA or RAR messages to enable event triggering.
Monitoring-Key	1066/ 10415	OctetString	SCE bucket ID	Identifies the monitoring control instance (bucket) that Usage-Monitoring-Information AVP refers to. Present in the Usage-Monitoring-Information AVP.
Usage-Monitoring-Information	1067/ 10415	Grouped	Grouped AVP	Appears when the Event-Trigger AVP is set to USAGE_REPORT.
Granted-Service-Unit	431	Grouped	Grouped AVP	Provides the threshold level to the PCEF. Present in the Usage-Monitoring-Information AVP.
Used-Service-Unit	446	Grouped	Grouped AVP	Provides the measured usage to the PCRF. Present in the Usage-Monitoring-Information AVP.
Usage-Monitoring-Level	1068/ 10415	Enumerated	PCC_RULE_LEVEL (1)	Supports only pre-defined PCC rule. Present in the Usage-Monitoring-Information AVP.
Usage-Monitoring-Report	1069/ 10415	Enumerated	Empty value USAGE_MONITORING_REPORT_REQUIRED (0)	Value of “0” indicates a request from the PCRF for a report of accumulated usage, regardless of whether or not threshold has been reached. Present in the Usage-Monitoring-Information AVP.

Table A-10 Supported Gx RLS9 Messages and AVPs (continued)

AVP Name	AVP Code (Code / Vendor-Id)	Value Type	Value	Comment
Usage-Monitoring-Support	1070/ 10415	Enumerated	USAGE_MONITORING_ DISABLED (0)	Indicates that usage monitoring is disabled for the relevant monitoring key. Present in the Usage-Monitoring-Information AVP.
CC-Total-Octets	421	Unsigned64	Total volume in bytes (either threshold or actual).	Present in the Granted-Service-Unit AVP and the Used-Service-Unit AVP.
CC-Input-Octets	412	Unsigned64	Uplink volume in bytes (either threshold or actual).	Present in the Granted-Service-Unit AVP and the Used-Service-Unit AVP.
CC-Output-Octets	414	Unsigned64	Downlink volume in bytes (either threshold or actual).	Present in the Granted-Service-Unit AVP and the Used-Service-Unit AVP.

Usage-Monitoring-Information

The Usage-Monitoring-Information AVP is enabled when the value of the Event-Trigger AVP is USAGE_REPORT.

The SCE reports the accumulated usage under the following conditions:

- When a usage threshold is reached
- When a package (containing the predefined PCC rules) is changed
- When usage monitoring is explicitly disabled by the PCRF
- When the session is terminated
- When requested by the PCRF (by setting the value of USAGE_MONITORING_REPORT_ REQUIRED (0) in the Usage-Monitoring-Report AVP in an RAR or CCA message).

To report, the SCE sends a CCR message as follows:

- CC-Request-Type AVP = "UPDATE_REQUEST"
- Event-Trigger AVP = "USAGE_REPORT"
- Usage-Monitoring-Information AVP includes:
  - Monitoring key (SCA BB bucket ID) in the Monitoring-Key AVP
  - The accumulated usage since the last report in the Used-Service-Unit AVP (using CC-Total-Octets, CC-Input-Octets, or CC-Output-Octets).

Usage-Monitoring-Information AVP Format

```
<Usage-Monitoring-Information> ::= [ Monitoring-Key ]
                                  [ Grante-Service-Unit ]
                                      [ CC-Total-Octets ]
                                      [ CC-Input-Octets ]
                                      [ CC-Output-Octets ]
                                      *[ AVP ]
                                  [ Used-Service-Unit ]
                                      [ CC-Total-Octets ]
                                      [ CC-Input-Octets ]
                                      [ CC-Output-Octets ]
                                      *[ AVP ]
                                  [ Usage-Monitoring-Level ]
                                  [ Usage-Monitoring-Report ]
                                  [ Usage-Monitoring-Support
```

APPENDIX B

Supported VSAs

Revised: March 29, 2012, OL-24167-04

List of Supported VSAs

Table B-1 lists the supported VSAs.

Table B-1 Supported VSAs

AVP Name	AVP Code	Vendor Id	From Gx	Used in				Value Type	AVP Flag in CCR			
				RAR	RAA	CCR	CCA		V	M	P	May Encr.
3GPP-Charging-Characteristics	13	10415	x	—	—	O_C	—	UTF8String	x	x	—	—
3GPP-CG-Address	4	10415	x	—	—	O_C	-	Address	x	x	—	—
CG-Address	846	10415	x	—	—	O_C	-	Address	x	x	—	—
3GPP-Charging-Id	2	10415	x	—	—	O_C	-	Unsigned32	x	x	—	—
3GPP-GGSN-Address-Code-7	7	10415	x	—	—	O_C	-	Address	x	x	—	—
3GPP-GGSN-MCC-MNC	9	10415	x	—	—	O_C	-	UTF8String	x	x	—	—
3GPP-GPRS-QoS-Negotiated-Profile	5	10415	x	—	—	O_C	-	UTF8String	x	x	—	—
3GPP-IMEISV	20	10415	x	—	—	O_C	-	UTF8String	x	x	—	—
3GPP-IMSI	1	10415	x	—	—	O_C	-	UTF8String	x	x	—	—
3GPP-MS-TimeZone	23	10415	x	—	—	O_C	-	OctetString	x	x	—	—
3GPP-NSAPI	10	10415	x	—	—	O_C	-	UTF8String	x	x	—	—
3GPP-PDP-Type	3	10415	x	—	—	O_C	-	Unsigned32	x	x	—	—
3GPP-RAT-Type	21	10415	x	—	—	O_C	-	OctetString	x	x	—	—
3GPP-Selection-Mode	12	10415	x	—	—	O_C	-	UTF8String	x	x	—	—
3GPP-SGSN-Address-Code-6	6	10415	x	—	—	O_C	-	Address	x	x	—	—
3GPP-SGSN-MCC-MNC	18	10415	x	—	—	O_C	-	UTF8String	x	x	—	—
3GPP-User-Location-Info	22	10415	x	—	—	O_C	-	OctetString	x	x	—	—
3GPP-GGSN-Address	847	10415	x	—	—	O_C	-	Address	x	x	—	—

Table B-1 Supported VSAs (continued)

AVP Name	AVP Code	Vendor Id	From Gx	Used in				Value Type	AVP Flag in CCR			
				RAR	RAA	CCR	CCA		V	M	P	May Encr.
3GPP-SGSN-Address	1228	10415	x	—	—	O_C	—	Address	x	x	—	—
3GPP2-Home-Agent-IP-Address	7	5535	—	—	—	—	—	Address	—	—	—	—
3GPP2-ESN	52	5535	—	—	—	—	—	OctetString	—	—	—	—
3GPP2-MEID	116	5535	—	—	—	—	—	OctetString	—	—	—	—
3GPP2-BSID	10	5535	—	—	—	—	—	OctetString	—	—	—	—
3GPP2-IP-Technology	22	5535	—	—	—	—	—	Uint32	—	—	—	—
3GPP2-PCF-IP-Address	9	5535	—	—	—	—	—	Address	—	—	—	—
Acct-Multi-Session-ID	50	—	x	—	—	O_C	—	UTF8String	—	x	—	—
Acct-Session-ID	44	—	x	—	—	O_C	—	UTF8String	—	x	—	—
Acct-Session-Time	46	—	x	—	—	O_C	—	Unsigned32	—	x	—	—
Called-Station-ID	30	—	x	—	—	O_C	—	OctetString	—	x	—	—
Calling-Station-ID	31	—	x	—	—	O_C	—	—	—	x	—	—
Class	25	—	x	—	—	O_C	—	OctetString	—	x	—	—
CUI	89	—	x	—	—	O_C	—	UTF8String	—	x	—	—
Framed IP Address	8	—	x	—	—	O_C	—	Address	—	x	—	—
NAS-Identifier	32	—	x	—	—	O_C	—	OctetString	—	x	—	—
NAS-IP-Address	4	—	x	—	—	O_C	—	Address	—	x	—	—
NAS-Port-Type	61	—	x	—	—	O_C	—	Unsigned32	—	x	—	—
Sub-OS-Info-Map	9	1071	—	—	—	—	—	UTF8String	—	—	—	—
User-Name	1	—	x	—	—	O_C	—	OctetString	—	x	—	—
WiMax-Active-Time	39	24757	—	—	—	O_C	—	Unsigned32	x	x	—	—
WiMax-BSID	46	24757	—	—	—	O_C	—	UTF8String	x	x	—	—