CHAPTER 4

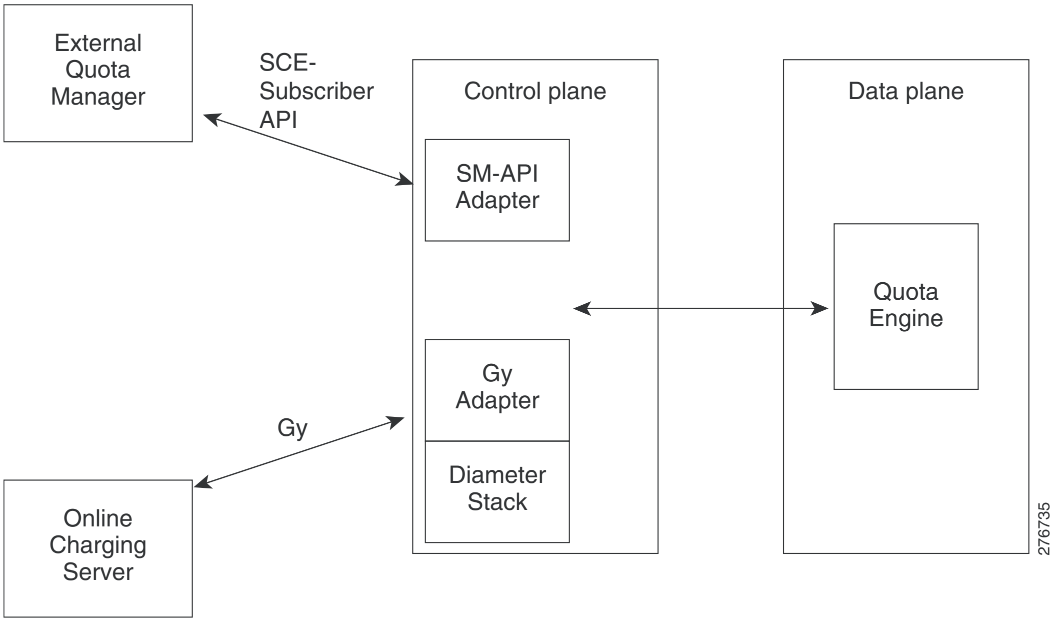
Gy Interface Support

Published: December 23, 2013

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.

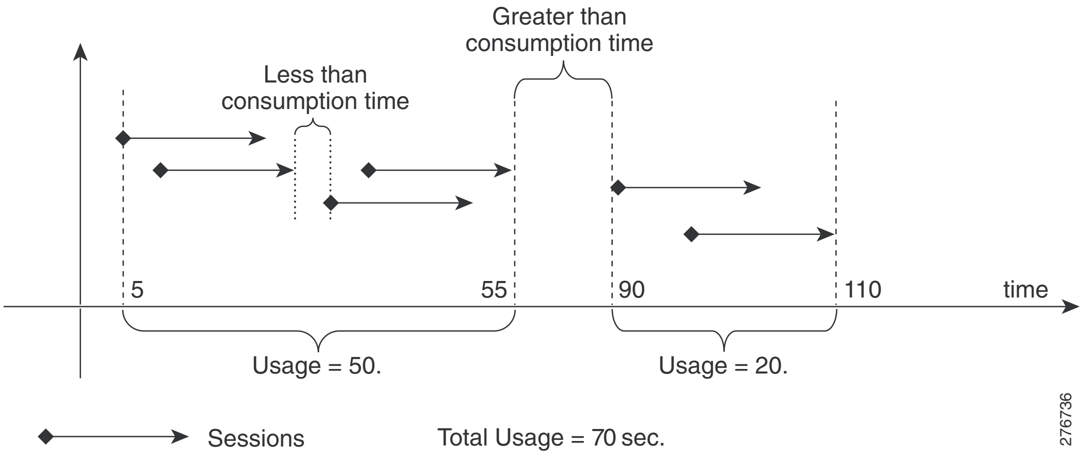
For additional Gy quota information, see the following sections:

- 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

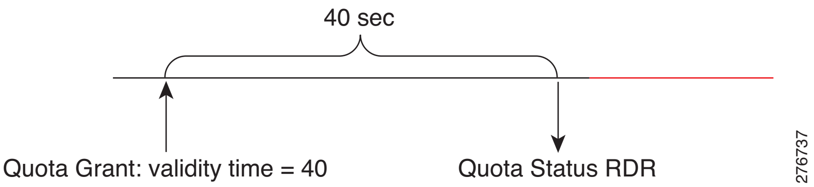
The supported quota timers are the Quota Validity Time and the Quota Holding Time.

- 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.

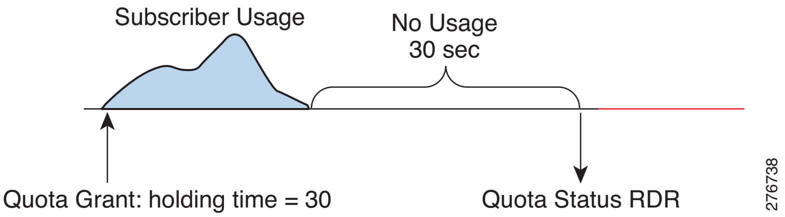
After the quota validity time expires, the SCE sends a Quota Status RDR and invalidates the bucket quota. It is the responsibility of the server to update the bucket quota and the action again. If the server does not respond, the bucket state is changed to error and an error action is applied to all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

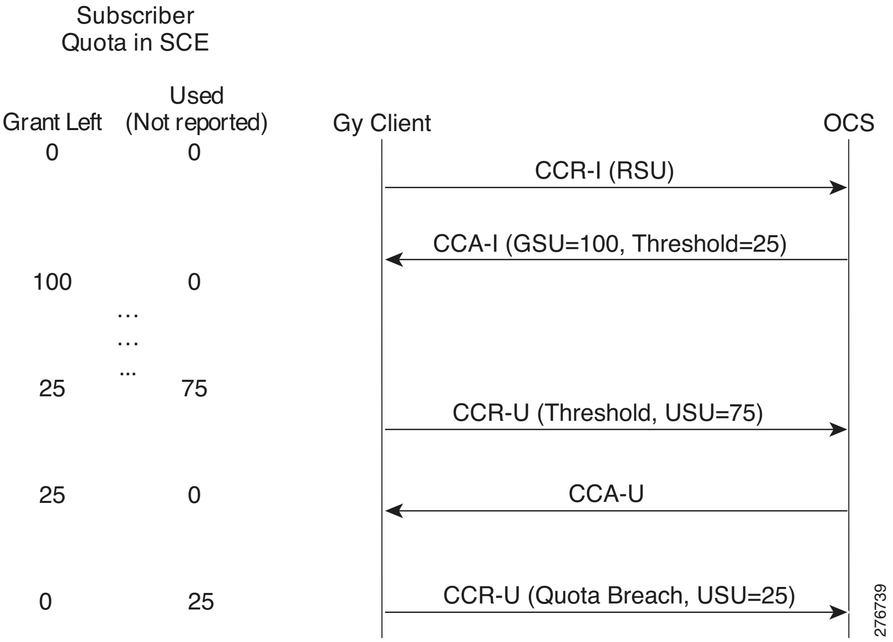
Tariff Time Change

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).

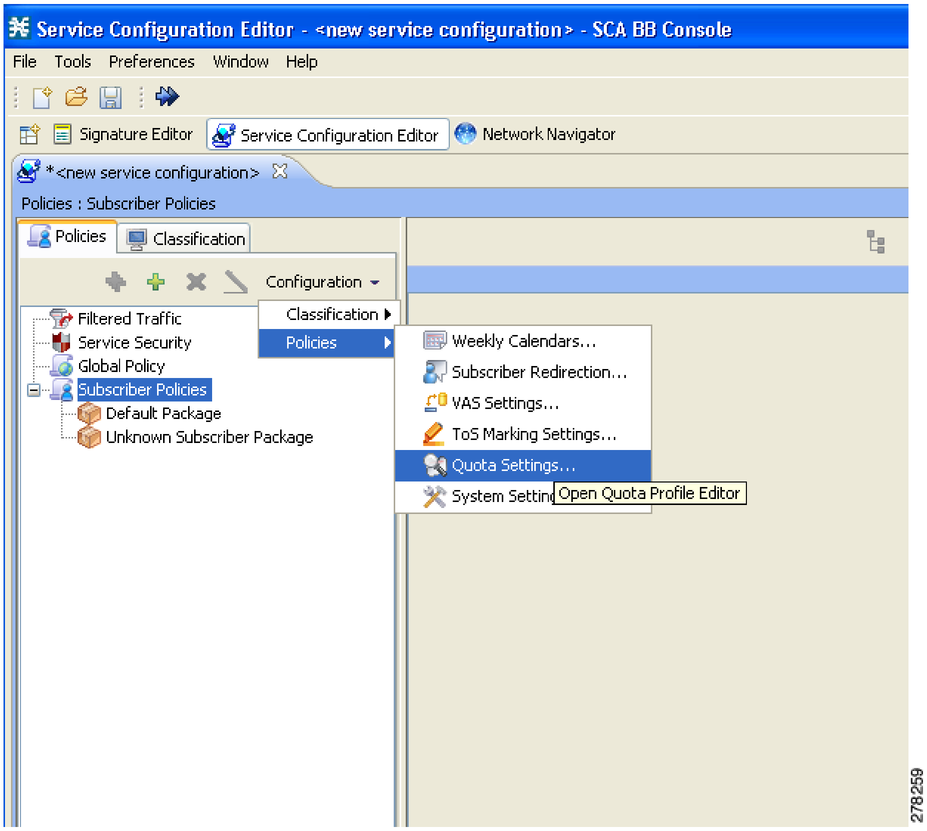
Step 4 Assign the profile to the appropriate package (Attaching the Quota Profile to a Package, page 4-17).

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



Global Quota Configuration

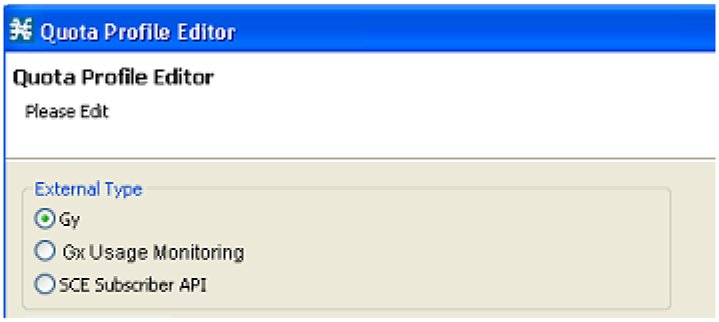
There are two aspects of global quota configuration:

- 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

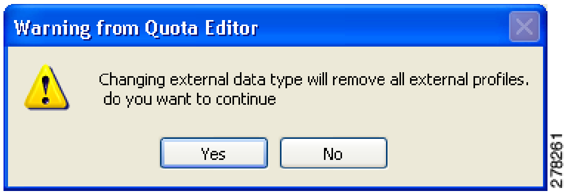
● Gy

○ 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



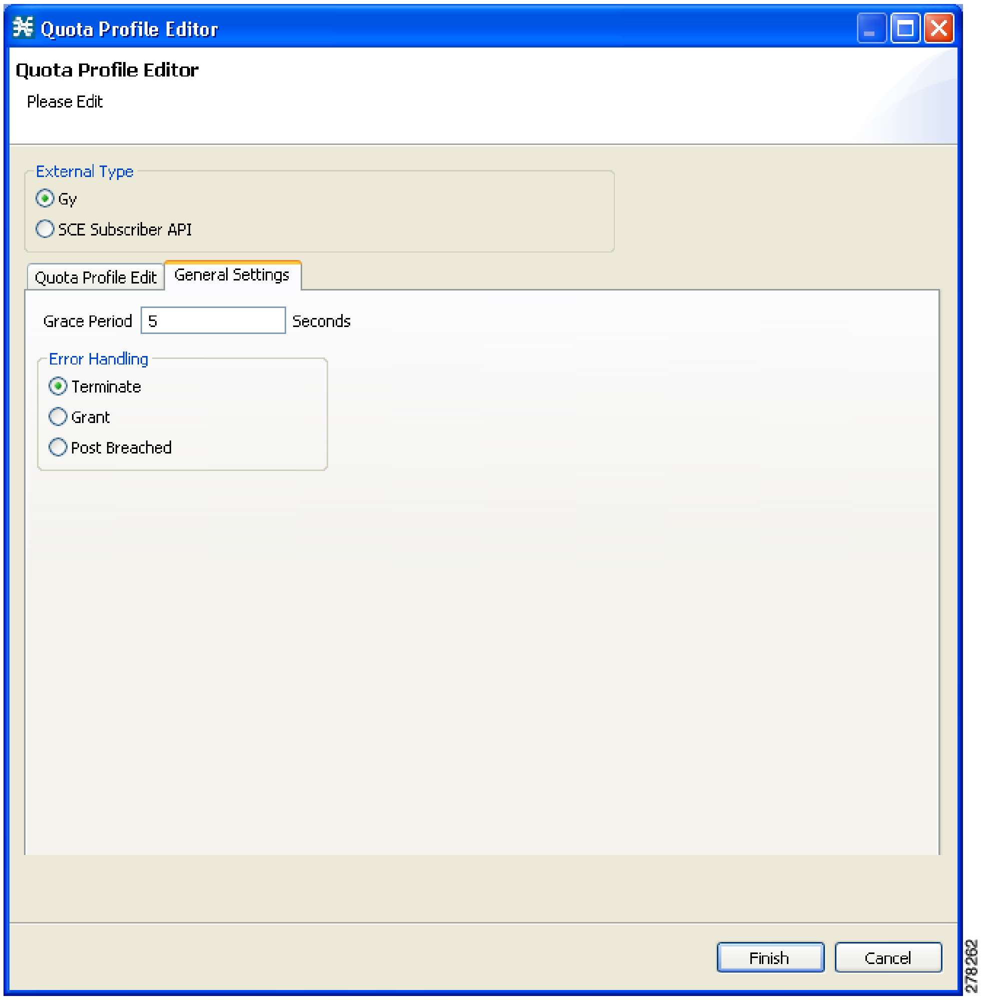
Warning from Quota Editor

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



Quota Profile Editor

Please Edit

External Type

● Gy

○ SCE Subscriber API

Grace Period 5 Seconds

Error Handling

● Terminate

○ Grant

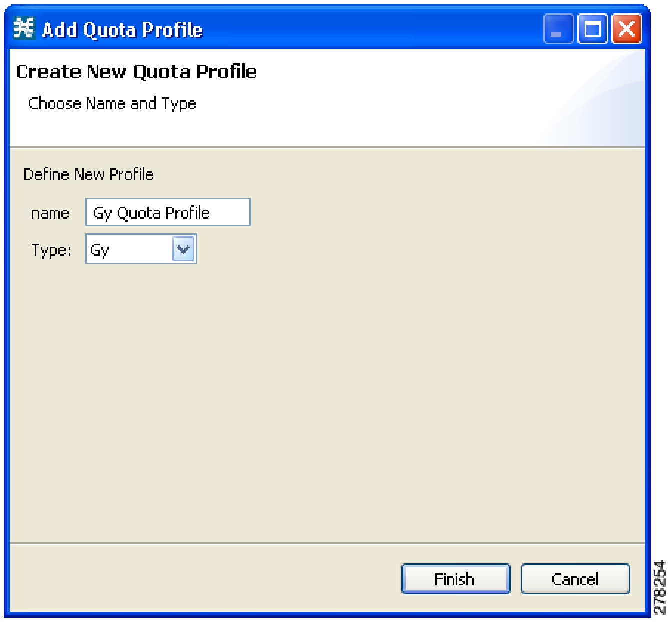
○ Post Breached

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.

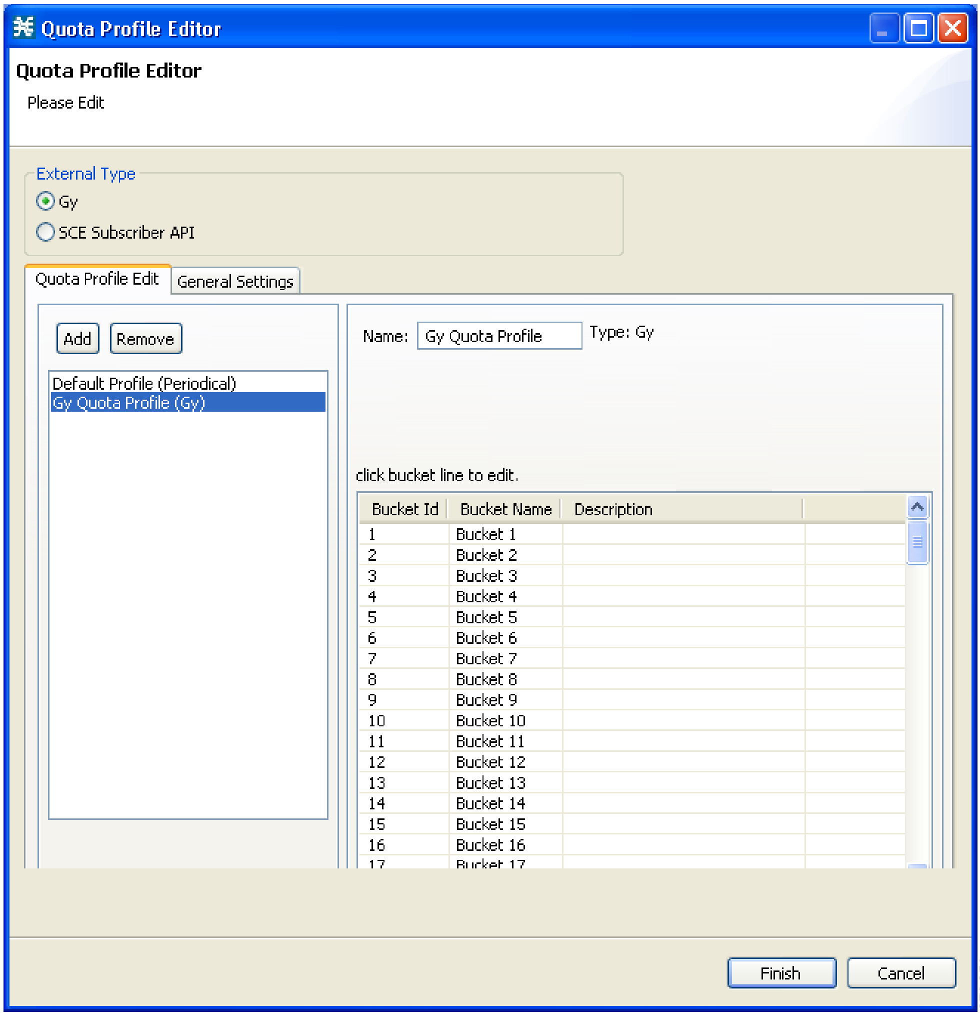
Note You cannot edit the default profile.

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

Please Edit

External Type
● Gy
○ SCE Subscriber API

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	

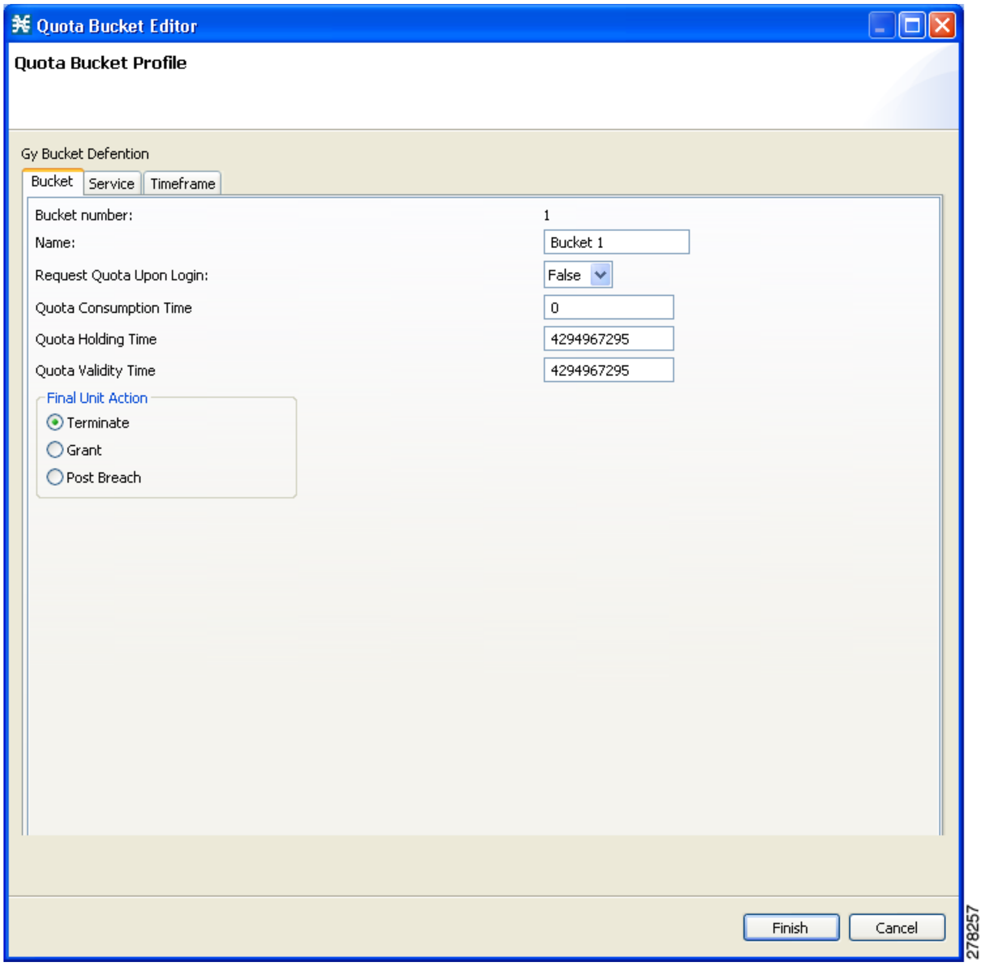
Step 2 Double-click the desired bucket to edit it.

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



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

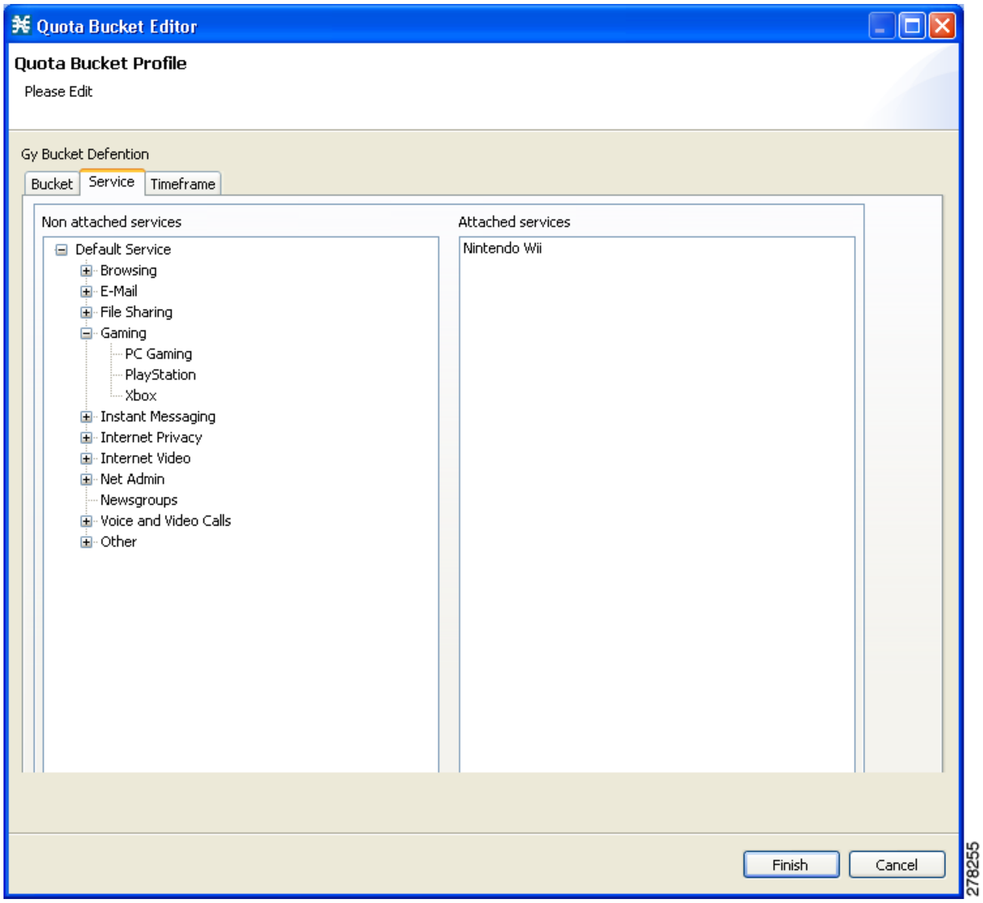
● Terminate
○ Grant
○ Post Breach

- 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.

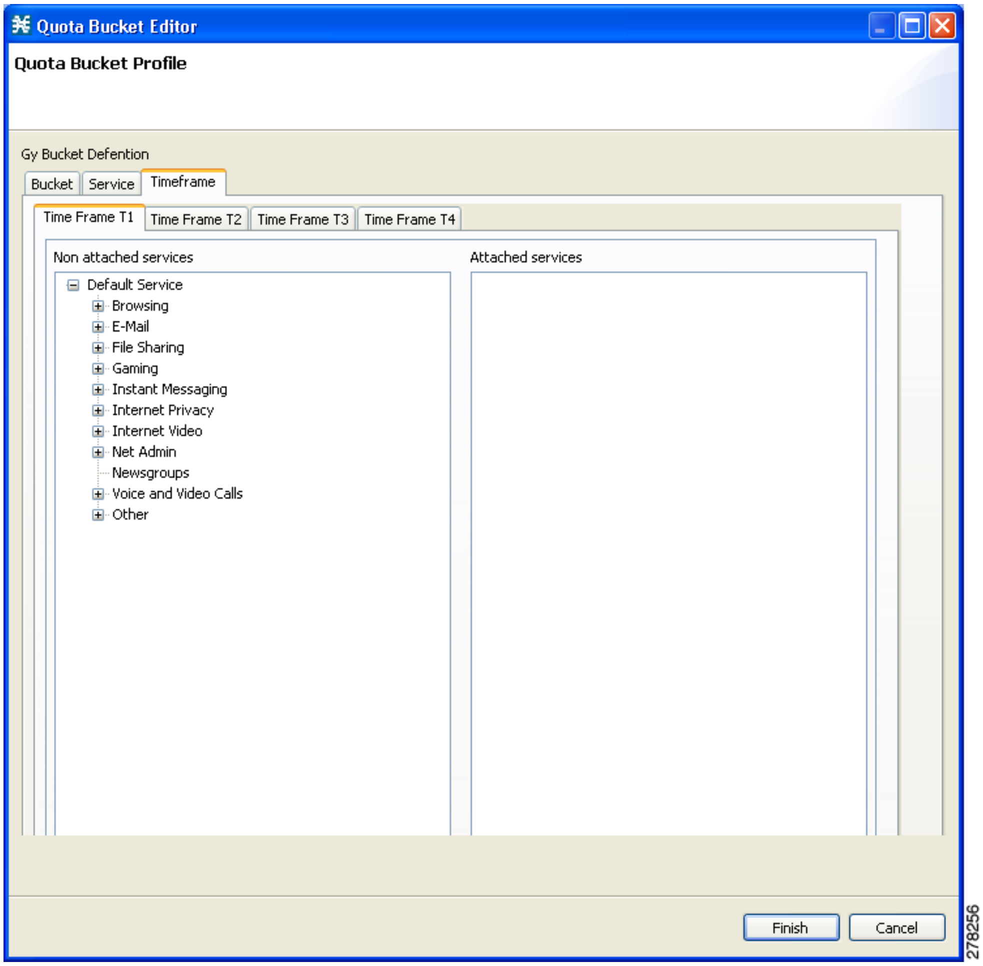
    If you drag a service, all its subservices in the tree are dragged as well.

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



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:

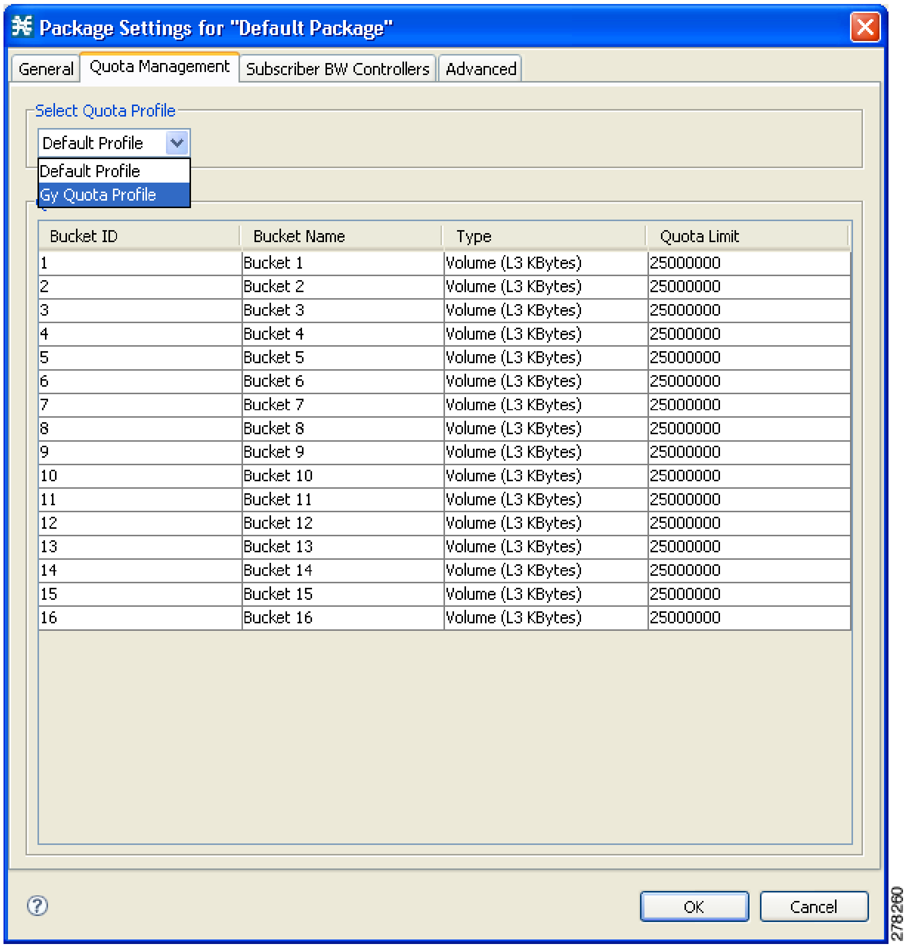
Step 1 Right-click the package in the **Policies** tab of the Service Configuration window to access the Package Settings screen.

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



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.**

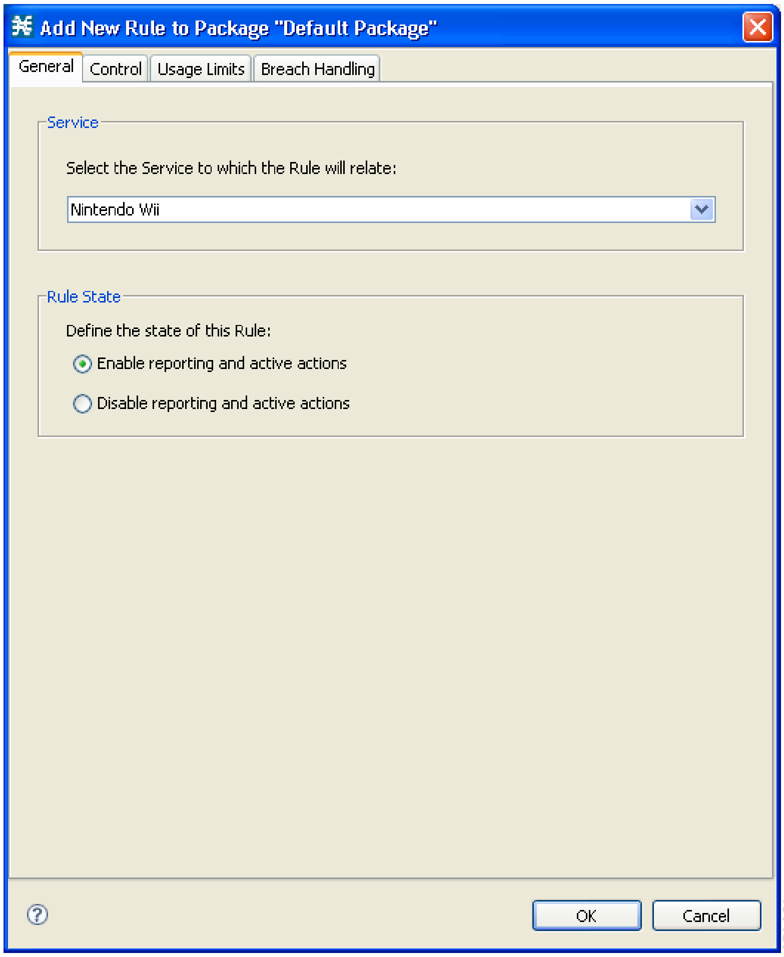
Defining a Rule Using the Quota Profile

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

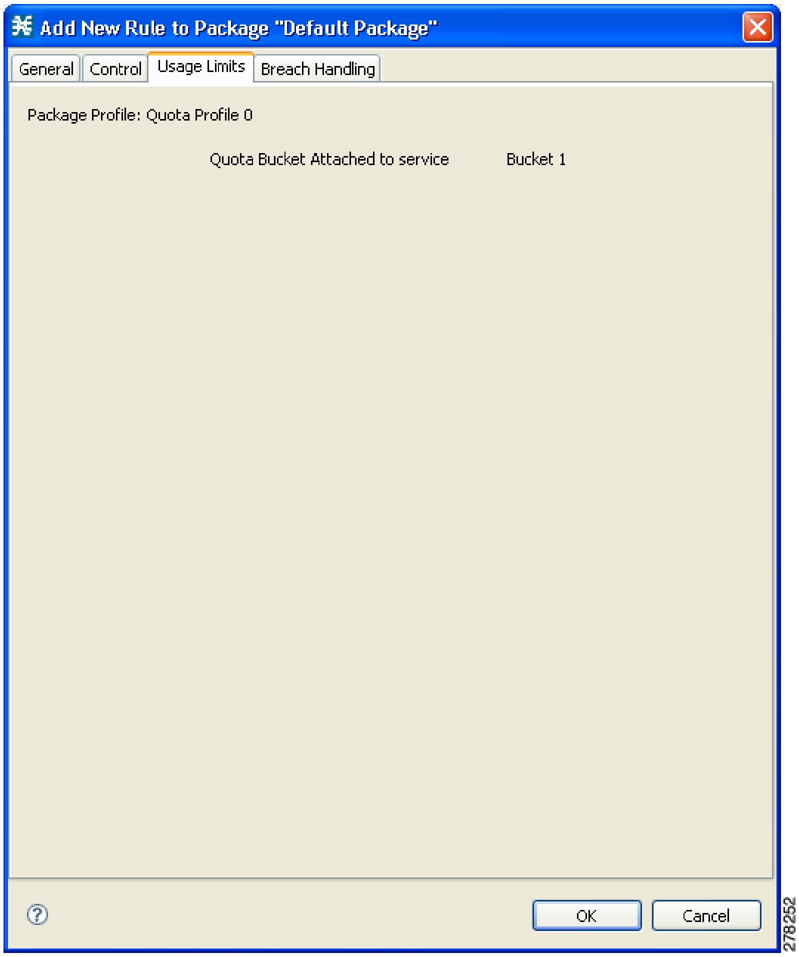
Define the state of this Rule:

● 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 3-9, and the following sections:

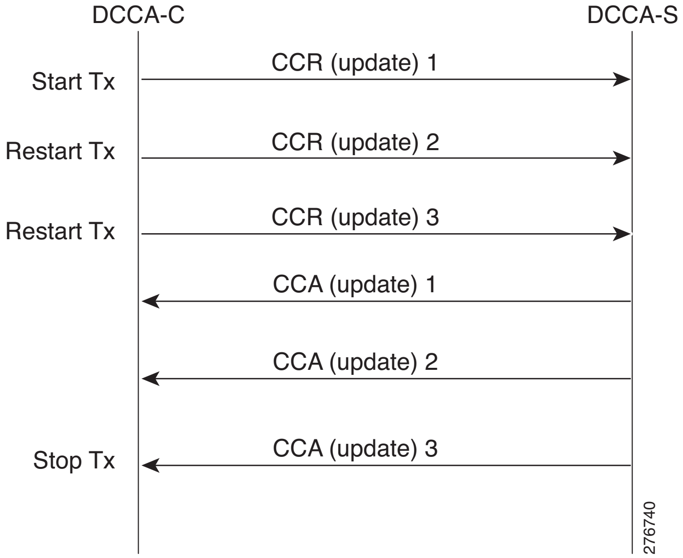
- Tx Timer, page 4-22
- CCSF, page 4-23
- CCFH, page 4-24
- Gy Failover Decisions, page 4-24
- Failure Handling of an Initial CCR Message, page 4-25
- Failure Handling of an Updated CCR Message, page 4-25
- DCCA Event Tables, page 4-25
- Detailed Flow Charts for Failover Scenarios, page 4-30
- Cascade 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 but the credit control server instructs the Cisco SCE not to send any requests for quota.

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.
CC initial answer received with result code equal to DIAMETER_CREDIT_LIMIT_REACHED		Notify “Final Unit Action” to SCA BB if final unit indication is set. If final unit indication is not set, notify “Breach Handling” to SCA BB”.

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

	Action	
Event	SCA BB	Gy Client
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
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.

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

	Action	
Event	**SCA BB**	**Gy Client**
User Logout	SCA BB sends Status Termination RDR	—
	—	Gy interface sends CC Terminate.
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

Event	Action	
	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

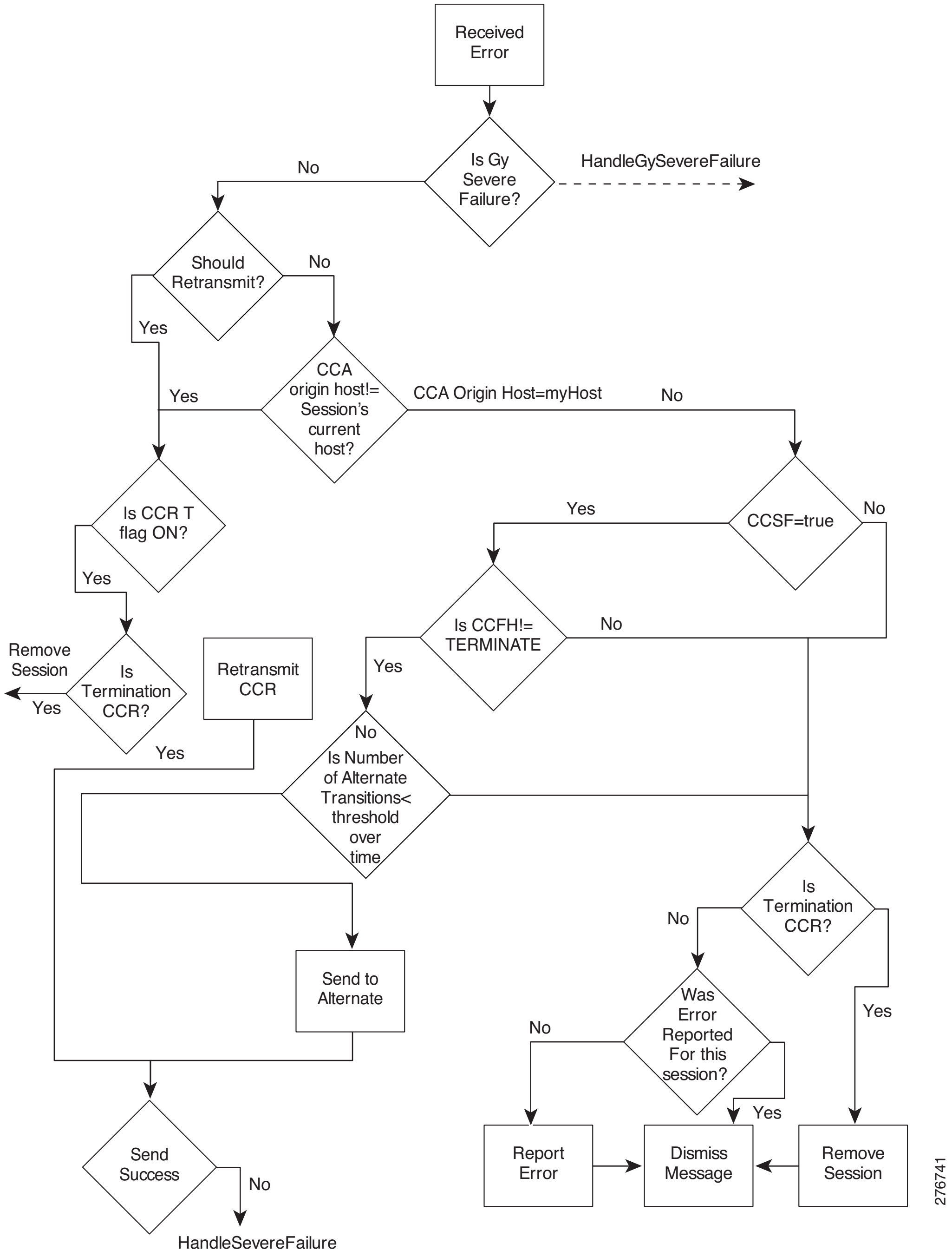
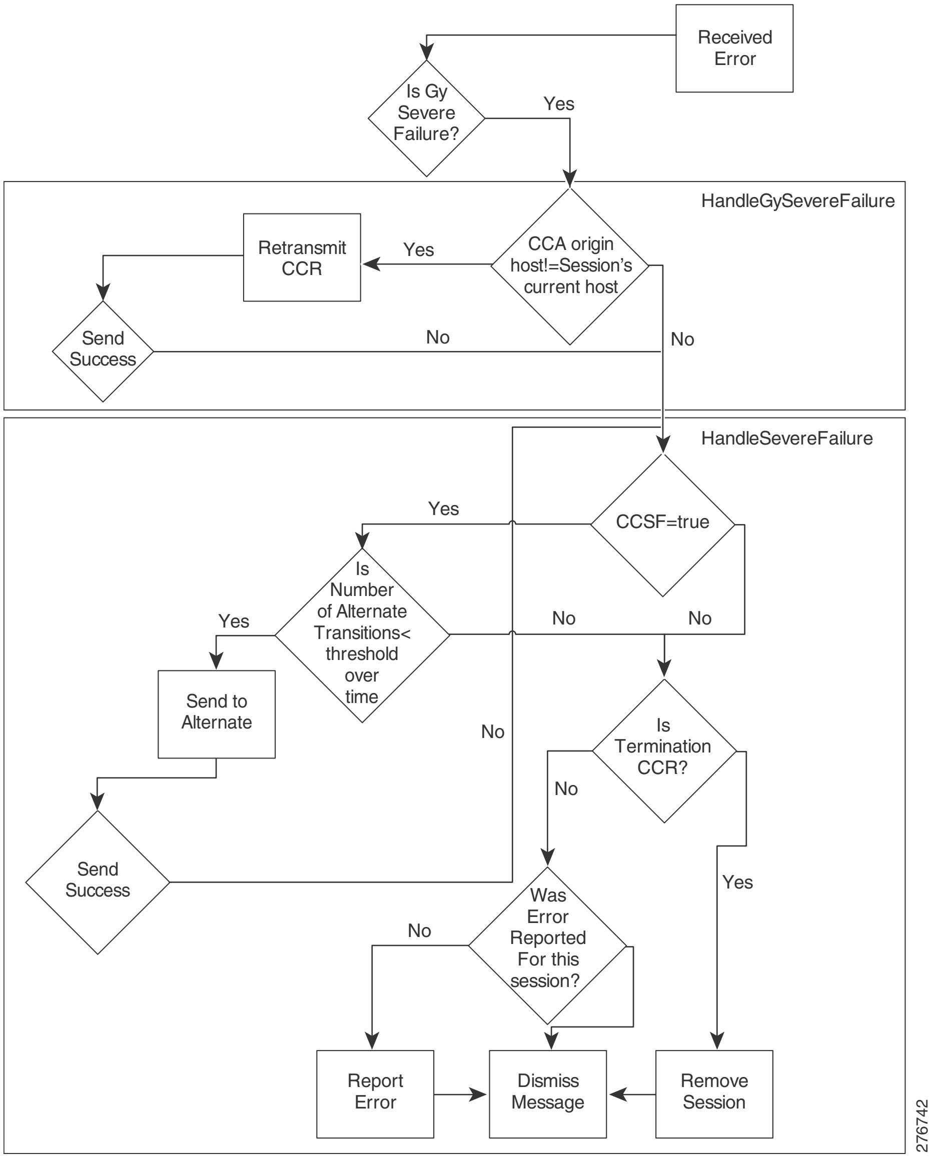


Figure 4-20 depicts the Gy client behavior upon severe failure situation.

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.