CHAPTER 8

Implementing Enhanced Service-Aware Billing

This chapter describes how to implement the Cisco Gateway GPRS Support Node (GGSN) as a service-aware GGSN. A service-aware GGSN is capable of real-time credit-control for prepaid subscribers and service-aware billing for postpaid and prepaid subscribers.

Note Service-aware GGSN functionality is supported for IPv4 packet data protocol (PDP) contexts only.

For complete descriptions of the GGSN commands in this chapter, see *Cisco GGSN Command Reference* for the Cisco GGSN release you are using. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

This chapter includes the following sections:

- Service-Aware GGSN Overview, page 8-2
- Reviewing Limitations and Restrictions, page 8-3
- Enabling Support for Service-Aware Billing, page 8-3
- Configuring Wait Accounting, page 8-4
- Configuring the GGSN to Generate Enhanced G-CDRs, page 8-4
- Configuring Quota Server Support on the Cisco GGSN, page 8-5
- Implementing Service-Aware Billing with Diameter/DCCA Support, page 8-12
- Implementing Service-Aware Billing with OCS Address Selection Support, page 8-29
- Enabling PCC under an APN, page 8-31
- Configuring Standalone GGSN Prepaid Quota Enforcement, page 8-32
- Configuring the Charging Record Type under an APN, page 8-34
- GTP-Session Redundancy for Service-Aware PDPs Overview, page 8-35
- Configuring Per-Service Local Sequence Number Synchronization, page 8-36
- Configuring Activity-Based Time Billing for Prepaid Subscribers, page 8-36
- Configuring HTTP Redirection, page 8-37
- Configuring Cisco CSG2 Load Balancing, page 8-43
- Reviewing Trigger Conditions for Enhance Quota Server Interface Users, page 8-45
- Configuration Examples, page 8-47

Service-Aware GGSN Overview

Implemented together, Cisco GGSN and Cisco Content Services Gateway - 2nd Generation (CSG2) function as a service-aware GGSN, also known as an enhanced GGSN (eGGSN).

There are two methods of implementing a service-aware GGSN:

1. Using the Cisco GGSN and Cisco CSG2 configuration with Cisco IOS Diameter protocol/Diameter Credit Control Application (DCCA) support on the GGSN
2. Using Cisco GGSN and Cisco CSG2 configuration with Online Charging System (OCS) address support on the GGSN.

In a service-aware GGSN implementation, Cisco CSG2 and GGSN provide the following functions:

- Cisco CSG2:
  - Inspects packets and categorizes traffic.
  - Requests quota and reports usage.
  - Provides billing plans, service names, and content definitions.
  - Acts as a RADIUS proxy for non-DCCA traffic.
  - Functions in prepaid mode for each service-flow charge recording.

  For detailed information about configuring Cisco CSG2, see *Cisco Content Services Gateway - 2nd Generation Release 3.5 Installation and Configuration Guide*.
- When implemented with Diameter/DCCA, the GGSN:
  - Functions as a quota server to Cisco CSG2.
  - Provides the Diameter interface to the DCCA server for quota requests and returns.
  - Manages the quota requested by Cisco CSG2 and received from the DCCA server.
  - Maps DCCA server rulebases to Cisco CSG2 billing plans.
  - Maps DCCA server category quota to Cisco CSG2 service quota.
- When implemented with OCS address selection support, the GGSN functions as a quota server for postpaid subscribers only. OCS address selection support enables an external OCS to which Cisco CSG2 has a direct connection to provide online credit control for prepaid subscribers.

To implement a service-aware GGSN, complete the tasks in the following sections:

- Reviewing Limitations and Restrictions, page 8-3
- Enabling Support for Service-Aware Billing, page 8-3 (Required)
- Configuring Wait Accounting, page 8-4 (Required if support for service-aware billing is enabled on an access point name [APN])
- Configuring the GGSN to Generate Enhanced G-CDRs, page 8-4 (Required)
- Configuring Quota Server Support on the Cisco GGSN, page 8-5 (Required)
- Implementing Service-Aware Billing with Diameter/DCCA Support, page 8-12 (Required if OCS Address Selection Support is not enabled)
- Implementing Service-Aware Billing with OCS Address Selection Support, page 8-29 (Required if Diameter/DCCA Support is not configured)
- Configuring the Service Aware Billing Parameters in Charging Profiles, page 8-25 (Required)

Reviewing Limitations and Restrictions

The following limitations and restrictions apply to enhanced service-aware billing:

- If session redundancy is required, GGSN supports a maximum of 21 categories per user.
- To populate the Cisco CSG2 User Table entries with the PDP context user information, enable RADIUS accounting between the Cisco CSG2 and Cisco GGSN.
- Configure the quota server address of the Cisco GGSN on the Cisco CSG2.
- If using DCCA, configure the service IDs on Cisco CSG2 as numeric strings that match the category IDs on the DCCA server.
- If you are not using RADIUS, configure the Cisco CSG2 as a RADIUS proxy on the GGSN.
- On the SGSN, the values you configure for the number GTP N3 requests and T3 retransmissions must be larger than the sum of all possible server timers (RADIUS, DCCA, and Cisco CSG2).

  Specifically the SGSN N3*T3 must be greater than:

  2 x RADIUS timeout + *N* x DCCA timeout + Cisco CSG2 timeout

  where:

  - 2 is for both authentication and accounting.
  - *N* is for the number of Diameter servers configured in the server group.
- If you enable support for service-aware billing on an access point name (APN), configure the GGSN to wait for a RADIUS accounting response before sending a Create PDP Context response to the SGSN.

Enabling Support for Service-Aware Billing

Support for enhanced service-aware billing must be enabled on the GGSN before you can implement service-aware billing features on the Cisco GGSN.

To enable service-aware billing support on the GGSN, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs service-aware`	Enables the GGSN to support service-aware billing.

To enable service-aware billing support on a particular access-point, use the following command in access-point configuration mode:

Command	Purpose
`Router(access-point-config)# service-aware`	Enables an APN to support service-aware billing.

Note If you enable support for service-aware billing under an APN, you must configure the GGSN to wait for a RADIUS accounting response before it sends a Create PDP Context response to the SGSN. For information about configuring the GGSN to wait for a RADIUS accounting response, see the "Configuring Wait Accounting" section on page 8-4.

Configuring Wait Accounting

If service-aware billing is enabled under an APN, you must configure wait accounting on the GGSN. When wait accounting is configured on the GGSN, the waits for a RADIUS accounting response before it sends a Create PDP Context response to the SGSN

To enable wait accounting on the GGSN, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs gtp response-message wait-accounting`	Configures the GGSN to wait for a RADIUS accounting response before sending a Create PDP Context response to the SGSN.

Note Wait accounting is required for an enhanced GGSN (eGGSN) implementation, but is optional for a Standalone GGSN Quota Enforcement.

Configuring the GGSN to Generate Enhanced G-CDRs

Gateway GPRS support node-call detail records (G-CDRs) contain information for the entire duration of, or part of, a PDP context. The G-CDR includes information such as the subscriber (mobile station ISDN [MSISDN] number, mobile subscriber identity [IMSI]), APN used, Quality of Service (QoS) applied, SGSN ID (as the mobile access location), a time stamp and duration, the data volume recorded separately for the upstream and downstream direction, and volume thresholds for intermediate CDR generation and tariff time switches.

In addition, enhanced G-CDRs (eG-CDRs) also contain a service-record information element (IE) that contains the usage data of each service flow used by a PDP session, specified by category ID. For example, the upstream and downstream volume, and the duration are recorded per service flow.

By default, the GGSN does not include the service records in G-CDRs. To support a service-aware GGSN implementation, you must configure the GGSN to generate eG-CDRs by configuring it to include service records in G-CDRs.

Note With Cisco GGSN Release 9.2 and later, the generation of enhanced G-CDRs (eG-CDRs) requires that charging release 7 has been configured on the GGSN by using the **gprs charging release 7** command in global configuration mode.

To configure the GGSN to include the service records in G-CDRs, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs charging cdr-option service-record [1-100]`	Configures the GGSN to include the service-record IE in G-CDRs and specifies the maximum service records an G-CDR can contain before the G-CDR is closed and a partial G-CDR is opened. A valid value is a number between 1 and 100. The default is 5.

To configure the GGSN to include the public land mobile network (PLMN) ID, radio access technology (RAT), or User Location Info fields in the service-record IE in eG-CDRs, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs charging service-record include [plmn-id | rat | user-loc-info-change]`	Configures the GGSN to include certain fields in the service-record IE in eG-CDRs, where: • **plmn-id**—Configures the GGSN to include the PLMN-ID field. • **rat**—Configures the GGSN to include the RAT field. The RAT indicates whether the SGSN serves the user equipment (UE) UMTS or GSM/EDGE RAN (GERAN). • **user-loc-info-change**—Configures the GGSN to include the User-Location-Info field.

Configuring Quota Server Support on the Cisco GGSN

To configure quota server support on the GGSN, complete the tasks in the following sections:

- Configuring a Cisco CSG2 Server Group, page 8-6 (Required)
- Configuring the Quota Server Interface on the GGSN, page 8-7 (Required)
- Advertising the Next Hop Address For Downlink Traffic, page 8-10
- Configuring the GGSN to Use the Cisco CSG2 as a RADIUS Authentication and Accounting Proxy, page 8-10 (Required, if RADIUS is not being used.)
- Monitoring and Maintaining the Quota Server-to-CSG2 Configuration, page 8-12

Configuring a Cisco CSG2 Server Group

We recommend that you configure two Cisco CSG2s (one active, the other standby) to function as one when interacting with the quota server process on the GGSN.

When configuring the Cisco CSG2 group that the GGSN quota server interface uses to communicate with the Cisco CSG2, you must specify a virtual IP address along with the real IP addresses of each of the Cisco CSG2s that make up the redundant pair. The quota server process on the GGSN communicates with the virtual address and the active Cisco CSG2 listens to the virtual IP address.

To configure a Cisco CSG2 group on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# ggsn csg csg-group-name`	Specifies a name for the Cisco CSG2 server group and enters Cisco CSG2 group configuration mode.
Step 2	`Router(config-csg-group)# virtual-address ip-address`	Specifies the virtual IP address of the Cisco CSG2 group. This is the IP address that the quota server process on the GGSN uses to communicate with the Cisco CSG2.
Step 3	`Router(config-csg-group)# port port-number`	(Optional) Configures the port on which the Cisco CSG2 listens for communications from the quota server. The default is 3386. **Note** The Cisco CSG2 always sends messages to the quota server on port 3386.
Step 4	`Router(config-csg-group)# real-address ip-address`	Configures the IP address of a real Cisco CSG2 for source checking of inbound messages from a Cisco CSG2. Configure a real IP address for each of the Cisco CSG2s that make up the redundant pair.
Step 5	`Router(config-csg-group)# aaa-group accounting server-group`	Configures the Cisco CSG2 RADIUS interface for accounting services.

Configuring the Quota Server Interface on the GGSN

In releases before Cisco GGSN Release 9.2, the GGSN uses the quota server interface to the Cisco CSG2 to obtain usage information to generate eG-CDRs for the following types of users:

- Service-aware prepaid (Gy) and service-aware postpaid (QS) users

  For prepaid subscribers or for postpaid subscribers configured as prepaid on the CSG2, the GGSN functions as the quota server and adds service containers to the eG-CDRs whenever it receives usage from the CSG2 over the quota server interface.

With Cisco GGSN Release 9.2 and later, you can specify the **service-msg** keyword option of the **ggsn quota-server** command to configure an enhanced quota server interface between the GGSN and Cisco CSG2. An *enhanced* quota server interface supports the exchange of service control messages that contain service usage information and enable the GGSN to generate eG-CDRs for the following additional types of users:

- Service-aware prepaid (GTP') users

  In a service-aware GGSN implemented with OCS address selection, the GGSN does not function as a quota server for prepaid users. OCS address selection support enables the Cisco CSG2 to obtain quota from an external OCS to which it has a direct GTP' connection. The GGSN generates eG-CDRs by obtaining the service usage via the enhanced quota server interface.

- Service-aware postpaid users

  The GGSN does not function as the quota server for service-aware postpaid users. The GGSN uses the enhanced quota server interface to obtain usage from the Cisco CSG2 and adds the usage to the eG-CDRs.

- Policy and Charging Control (PCC)-enabled (Gx) users

  When Gx-enabled users are also prepaid (Gy) users, support for eG-CDR generation is as present in releases before Cisco IOS Release 12.4(22)YE2 and the service containers are added to eG-CDRs based on the usage received in quota server messages.

  When a Gx user is also a prepaid user in an implementation in which the CSG2 has a direct OCS interface, or a postpaid user (either service-aware or nonservice-aware), the GGSN obtains usage from the CSG2 via the enhanced quota server interface and add the usage to the eG-CDRs.

Note With Cisco IOS Release 12.4(22)YE2 and later, when an enhanced quota server interface is enabled on the GGSN, the GGSN does not function as the quota server for service aware postpaid users or Gx postpaid users; therefore, these uses must be configured as postpaid on the Cisco CSG2. For information about configuring the Cisco CSG2, see *Cisco Content Services Gateway 2nd Generation - Release 3.5 Installation and Configuration Guide.*

Quota Server Interface

The quota server interface on the GGSN provides support of the following:

- Attributes in RADIUS Accounting Start messages to the Cisco CSG2
  - Billing plan ID—Corresponds with the rulebase ID received from a DCCA server. The quota server process on the GGSN maps the rulebase ID to the billing plan ID.
  - Quota server address and port—IP address and port of the quota server that the Cisco CSG2 should use for a user.
  - By default, this is the IP address of the GGSN unless OCS address selection support is enabled on the GGSN. For information about enabling OCS address selection support on the GGSN, see the "Implementing Service-Aware Billing with OCS Address Selection Support" section on page 8-29.
  - Downlink next hop address—Next hop address (user address) for downlink traffic (Cisco CSG2-to-GGSN).
- Threshold Limit Values (TLVs):
  - Quota Consumption Timer (QCT). The QCT is assumed to be zero.
  - Quota Holding Timer (QHT)
  - Quota Threshold

For more information on the quota server interface, billing plans, and the QCT and QHT, see *Cisco Content Services Gateway 2nd Generation - Release 3.5 Installation and Configuration Guide*.

Enhanced Quota Server Interface

The enhanced quota server interface provides the additional support the following:

- Service control messages
  - Service Control Request (SCR)
  - Service Control Request Ack
  - Service Control Usage (SCU)
  - Service Control Usage Ack
- Attributes in RADIUS Accounting and Stop messages to the Cisco CSG2
  - Quota server mode—Specifies the capability of the enhanced quota server interface; whether online charging is enabled or offline charging is enabled.
  - eG-CDR correlator ID—Identifier that the GGSN uses to match Service Control Usage with the Service Control Request

When configuring an enhance quota server interface:

- An APN must be enabled for service-aware billing support (**service-aware** command) or PCC-enabled (**pcc** command) to trigger service control messages.
- GPRS Charging Release 7 must be configured as described in the "Configuring the Charging Release" section on page 7-8.
- Configure a charging record type for participating APNs as described in the "Configuring the Charging Record Type under an APN" section on page 8-34.

- Configure the sychronization for per -service local sequence number as described in the "Configuring Per-Service Local Sequence Number Synchronization" section on page 8-36.
- You can configure one quota server interface per GGSN. Configuring more than one quota server interface overwrites the existing interface.

To configure the quota server interface on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# ggsn quota-server server-name [service-msg]`	Enables the quota server process on the GGSN and enters quota server configuration mode. Optionally, specify the **service-msg** keyword option to enable the quota server process to exchange service control messages.
Step 2	`Router(config-quota-server)# interface interface-name`	Specifies the logical interface, by name, for the quota server to use. We recommend that you use a loopback interface as the quota server interface. **Note** The quota server must use a different address than the GTP virtual template address.
Step 3	`Router(config-quota-server)# echo-interval [ 0 | 60-65535]`	Specifies the number of seconds that the quota server waits before sending an echo request message to the Cisco CSG. The valid values are 0 (echo messages are disabled) or a value between 60 and 65535. The default is 60.
Step 4	`Router(config-quota-server)# n3-requests number`	Specifies the maximum number of times that the quota server attempts to send a signaling request to the Cisco CSG. The valid value is a number between 2 and 65535. The default is 5.
Step 5	`Router(config-quota-server)# t3-response number`	Specifies the initial time that the quota server waits before resending a signaling request message when a response to a request has not been received. The valid value is a number between 2 and 65535. The default is 1.
Step 6	`Router(config-quota-server)# csg group csg-group-name`	Specifies the Cisco CSG2 group that the quota server process uses to communicate with a Cisco CSG2. **Note** The quota server process supports only one path to a Cisco CSG2, therefore, you can specify only one Cisco CSG2 group at a time. **Note** The the **csg group** quota server configuration command and the **csg-group** access point configuration command are mutually exclusive. You cannot define a CSG group under the quota server interface if one has already been configured under an APN.

	Command	Purpose
Step 7	`Router(config-quota-server)# scu-timeout` *csg-group-name*	Specifies the time, in seconds, that the GGSN waits to receive the SCU from the Cisco CSG2 before discarding the SCR. A valid value is a number between 1 and 1000. The default is 30.
Step 8	`Router(config-quota-server)# exit`	Exits quota server configuration mode.

Advertising the Next Hop Address For Downlink Traffic

To configure the next hop address (the user address) for downlink traffic (Cisco CSG2-to-GGSN) to be advertised in Accounting Start requests to the RADIUS endpoint, use the following command in access-point configuration mode:

Command	Purpose
`GGSN(access-point-config)# advertise downlink next-hop` *ip-address*	Configures the next hop address, to which downlink traffic destined for the GGSN is routed, to be advertised in Accounting Start requests.

Configuring the GGSN to Use the Cisco CSG2 as a RADIUS Authentication and Accounting Proxy

If you are not using RADIUS, you must configure the Cisco CSG2 as a RADIUS proxy.

To configure the GGSN to use the Cisco CSG2 as a RADIUS proxy, complete the following tasks:

- Configuring a Global RADIUS Server, page 8-11
- Configuring an AAA RADIUS Server Group that includes the Cisco CSG2, page 8-11
- Using Method List to Specify Supported Services, page 8-11
- Specifying Method Lists for an APN, page 8-12

Configuring a Global RADIUS Server

To configure a RADIUS server globally, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number]`	Specifies a RADIUS server host.
Step 2	`Router(config)# radius-server key {0 string | 7 string | string}`	Sets the authentication and encryption key for all RADIUS communications between the GGSN and the RADIUS daemon.

Configuring an AAA RADIUS Server Group that includes the Cisco CSG2

To define an Authentication, Authorization and Accounting (AAA) RADIUS server group, and include the Cisco CSG2 as a server in the server group, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa group server radius group-name`	Specifies an AAA RADIUS server group and assigns the selected server group for authentication services.
Step 2	`Router(config-sg-radius)# server ip_address [auth-port port-number] [acct-port port-number]`	Configures the IP address of the RADIUS endpoint in the server group.
Step 3	`Router(config-sg-radius)# exit`	Exits server group configuration mode.

Using Method List to Specify Supported Services

To use AAA method lists to specify the types of services the group supports, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa authentication ppp list-name group group-name`	Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP.
Step 2	`Router(config)# aaa authorization network list-name group group-name`	Sets parameters that restrict network access to a user.
Step 3	`Router(config)# aaa accounting network list-name start-stop group group-name`	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS.

Specifying Method Lists for an APN

To reference method lists for the APNs that use the Cisco CSG2 as a RADIUS proxy, use the following commands in access-point configuration mode:

	Command	Purpose
Step 1	`Router(access-point-config)# aaa-group authentication` *server-name*	Specifies an AAA server group and assigns the selected server group for authentication services on the access point.
Step 2	`Router(access-point-config)# aaa-group accounting` *server-name*	Specifies the logical interface, by name, for the quota server to use.

Monitoring and Maintaining the Quota Server-to-CSG2 Configuration

To monitor and maintain the quota server-to-Cisco CSG2 configuration, use the following commands in privileged EXEC mode.

Command	Purpose
`Router# clear ggsn quota-server statistics`	Clears quota server-related statistics (messages and error counts).
`Router# show ggsn quota-server [parameters | statistics]`	Displays quota server parameters or statistics about quota server messages and error counts.
`Router# show ggsn csg [parameters | statistics]`	Displays the parameters used by the Cisco CSG2 group or the number of path and quota management messages sent and received by the quota server.

Implementing Service-Aware Billing with Diameter/DCCA Support

To implement a service-aware GGSN with Diameter/DCCA support, complete the tasks in the following sections:

- Reviewing Service-Aware Billing with DCCA/Diameter, page 8-13
- Configuring the Diameter Base, page 8-16
- Configuring the DCCA Client Process on the GGSN, page 8-21
- Enabling Support for Vendor-Specific AVPs in DCCA Messages, page 8-24
- Configuring the Service Aware Billing Parameters in Charging Profiles, page 8-25

Reviewing Service-Aware Billing with DCCA/Diameter

In a service-aware GGSN implementation with DCCA, the Cisco CSG2 categorizes traffic, reports usage, and manages quota. The GGSN functions as a DCCA client to communicate with a DCCA server to provide the following functions:

- Diameter interface (Gy) to the DCCA server via which the Cisco CSG2 requests quota and reports usage.
- Quota negotiation by sending quota requests from the Cisco CSG2 to the DCCA server and pushing quota returns from the DCCA server to the Cisco CSG2.
- DCCA server rulebases to Cisco CSG2 billing plans mapping.
- DCCA server category quota to Cisco CSG2 service quota mapping.
- PDP maintenance and determining if a PDP is prepaid or postpaid.

If prepaid service-based charging or postpaid service-based charging is required, entries are created on the Cisco CSG2. The Cisco CSG2 inspects the service categories and reports usage to the GGSN. If the user is to be treated as a postpaid subscriber (offline charging), the GGSN records the usage information that is reported by the Cisco CSG2 in an eG-CDR. If the user is to be treated as a prepaid subscriber (online charging), the GGSN records the reported usage information in an eG-CDRs, and translates and sends the information to a DCCA server.

The GGSN also handles Gn-side triggers for quota reauthorization and server-initiated reauthorization or termination requests. The Cisco CSG2 sends the authorization requests, quota reports, and service stops to the GGSN,. The GGSN translates what the Cisco CSG2 sends into DCCA messages for transport over the Diameter interface. When the DCCA server responds with additional quota, the GGSN pushes the quota to the Cisco CSG2.

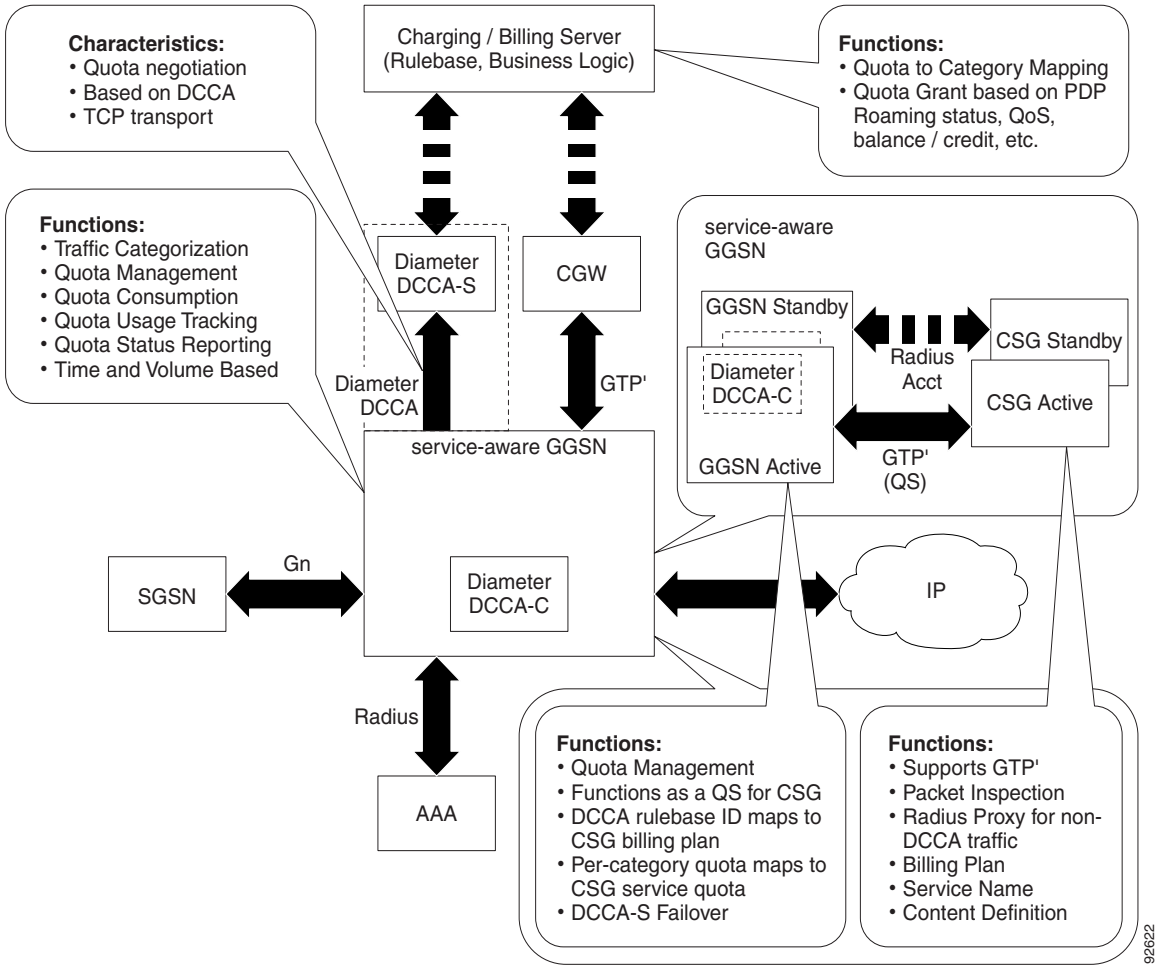
Note If RADIUS is not being used, you must configure the Cisco CSG2 as a RADIUS proxy.

This section contains the following overview information about service-aware billing with DCCA/Diameter:

- Supported Features, page 8-14
- Unsupported Features, page 8-15
- Messaging Support, page 8-15
- Service-Aware Billing with DCCA Data Flows, page 8-16

Figure 8-1 shows the functions and characteristics of a service-aware GGSN implemented with DCCA support.

Figure 8-1 High-Level Overview of Service-Aware GGSN Functions When Implemented with DCCA Support



Supported Features

To enable the implementation of a service-aware GGSN with DCCA, the Cisco GGSN supports the following features:

- Diameter/DCCA client interface support for online/real-time credit control for prepaid subscribers (IP PDP contexts only)
- Quota server functionality and interface to Cisco CSG2 for per-service billing
- Enhanced G-CDRs for service-based CDRs for prepaid and postpaid subscribers
- AAA authentication interface—DCCA rulebase support and charging profile selection
- AAA accounting interface—Cisco CSG2 User Table population and Cisco CSG-based proxies
- Enhanced Ga interface for offline charging

Unsupported Features

The following features are not supported by a service-aware GGSN implementation with DCCA:

- Charging differentiation for secondary PDP contexts
- PPP PDP contexts
- PPP regeneration
- Network management
- Cell identity
- PDP contexts for both online DCCA exchange and offline service-based usage
- Dynamic configuration for blocking/forwarding traffic while waiting for quota reauthorization
- Diameter proxy, relay, or redirection
- Diameter transport layer security
- SCTP transport
- No dual quota support (for receiving volume and time quota)

Messaging Support

To support credit control via Diameter, the DCCA client process on the GGSN and the DCCA server exchange the following messages:

- Credit Control Request (CCR)—Initial, Update, and Final
- Credit Control Answer (CCA)—Initial, Update, and Final

In addition, the GGSN Diameter interface supports the following base Diameter messages:

- Capability Exchange Request (CER) and Capability Exchange Answer (CEA)—The GGSN advertises DCCA support in CER messages. In addition, the GGSN can be configured to advertise support for vendor-specific attribute value pairs (AVPs) using the **diameter vendor support** command in global configuration mode.
- Disconnect Peer Request (DPR) and Disconnect Peer Answer (DPA)—The GGSN sends a DPR message when the CER with a Diameter peer fails or there is no Diameter server configured.
- Device Watchdog Request (DWR) and Device Watchdog Answer (DWA)—The GGSN uses DWR and DWA messages to detect transport failures with a Diameter peer. A watchdog timer can be configured for each Diameter peer using the **timer watchdog** command in Diameter peer configuration mode.
- Re-auth Request (RAR) and Re-auth Answer (RAA)
- Abort Session Request (ASR) / Abort Session Answer (ASA)—No Failed-AVP is sent in an ASA when an incorrect ASR is sent from the DCCA server.

As a DCCA client, the GGSN also receives the following notifications from Cisco IOS AAA:

- CCA message receipts
- Asynchronous session termination requests
- Server-initiated RARs

Service-Aware Billing with DCCA Data Flows

The following is a high-level overview of the flow of traffic during the creation of a PDP context for a prepaid subscriber in an enhanced service-aware billing implementation using DCCA.

PDP Context Creation Data Flow for Prepaid Subscribers

1. SGSN sends a Create PDP Context request to the service-aware GGSN.
2. GGSN sends an Access-Request message to the RADIUS (server or Cisco CSG2 configured as a RADIUS proxy).
3. RADIUS returns an Access-Accept response. From the Access-Accept response, the GGSN obtains a default rulebase ID, or if the response does not contain a default rulebase ID, the GGSN obtains the rulebase ID from a locally configured value in the charging profile selected for the Create PDP Context request.
4. Service-aware GGSN sends a Diameter Credit Control Request (CCR) to the DCCA server.
5. DCCA server returns a Credit Control Answer (CCA) to the GGSN. This CCA might contain a rulebase and quota request.
6. If the CCA contains a rulebase, the GGSN sends an Accounting-Start request with the selected rulebase to the RADIUS.
7. RADIUS receives the Accounting-Start request from the GGSN and creates a Cisco CSG2 User Table entry for the user.
8. RADIUS sends an Accounting-Start response to the GGSN.
9. If the DCCA server sends a quota request in a CCA to the GGSN, the GGSN pushes the quota request to the Cisco CSG2.
10. When the GGSN receives a quota push response from the Cisco CSG2, it sends the Create PDP Context response to the SGSN, and the context is established.

PDP Context Creation Data Flow for Postpaid Subscribers

1. SGSN sends a Create PDP Context request to the service-aware GGSN.
2. GGSN sends an Accounting-Start request containing the selected rulebase to the RADIUS (server or the Cisco CSG2 configured as a RADIUS proxy).
3. RADIUS proxy receives the Accounting-Start request and creates a Cisco CSG2 User Table entry for the user.
4. RADIUS proxy sends an Accounting-Start response to the GGSN.
5. When the GGSN receives the Accounting-Start response from the RADIUS proxy, it sends a Create PDP Context response to the SGSN, and the context is established.

Configuring the Diameter Base

To configure the Diameter protocol base, complete the tasks in the following sections:

- Configuring a Diameter Peer, page 8-17
- Enabling Diameter AAA, page 8-18
- Configuring Diameter Protocol Parameters Globally, page 8-19
- Monitoring and Maintaining the Diameter Base, page 8-21

Configuring a Diameter Peer

To configure a Diameter peer, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# diameter peer name`	Configures a device as a Diameter protocol peer and enters Diameter peer configuration mode.
Step 2	`Router(config-dia-peer)# address ipv4 ip-address`	Defines a route to the host of the Diameter peer using IPv4.
Step 3	`Router(config-dia-peer)# transport {tcp | sctp} port port-num`	Configures the transport protocol for connecting to the Diameter peer. **Note** The Cisco GGSN supports TCP.
Step 4	`Router(config-dia-peer)# security ipsec`	Configures IPSec as the security protocol for the Diameter peer-to-peer connection.
Step 5	`Router(config-dia-peer)# source interface interface`	Configures the interface to connect to the Diameter peer.
Step 6	`Router(config-dia-peer)# timer {connection | transaction | watchdog} value`	Configures Diameter base protocol timers for peer-to-peer communication. The valid range, in seconds, is from 0 to 1000. The default is 30. • **connection**—Maximum amount of time the GGSN attempts to reconnect to a Diameter peer after a connection to the peer is brought down due to a transport failure. A value of 0 configures the GGSN to not try to reconnect. • **transaction**—Maximum amount of time the GGSN waits for a Diameter peer response before trying another peer. • **watchdog**—Maximum amount of time the GGSN waits for a Diameter peer response to a watchdog packet. When the watchdog timer expires, a DWR is sent to the Diameter peer and the watchdog timer is reset. If a DWA is not received before the next expiration of the watchdog timer, a transport failure to the Diameter peer has occurred. When configuring timers, the value for the transaction timer, should be larger than the TX-timeout value, and, on the SGSN, the values configured for the number GTP N3 requests and T3 retransmissions must be larger than the sum of all possible server timers (RADIUS, DCCA, and Cisco CSG2). Specifically, the SGSN N3*T3 must be greater than 2 x RADIUS timeout + *N* x DCCA timeout + Cisco CSG2 timeout where: • 2 is for both authentication and accounting. • *N* is for the number of Diameter servers configured in the server group.

	Command	Purpose
Step 7	`Router(config-dia-peer)# destination host string`	Configures the Fully Qualified Domain Name (FQDN) of a Diameter peer.
Step 8	`Router(config-dia-peer)# destination realm string`	Configures the destination realm (part of the domain "@*realm*") of a Diameter peer. The realm might be added by the AAA client when sending a request to AAA. However, if the client does not add the attribute, then the value you configure in Diameter peer configuration mode is used when sending messages to the destination Diameter peer. If you do not configure a value in Diameter peer configuration mode, the value you configure globally by using the **diameter destination realm** command is used.
Step 9	`Router(config-dia-peer)# ip vrf forwarding name`	Associates a Virtual Routing and Forwarding (VRF) instance with a Diameter peer. **Note** If a VRF name is not configure for a Diameter server, the global routing table is used.

Enabling Diameter AAA

To enable Diameter AAA, complete the tasks in the following sections:

- Defining the Diameter AAA Server Group, page 8-18
- Defining an Authorization Method List for Prepaid Subscribers, page 8-19

Defining the Diameter AAA Server Group

For redundancy, configure Diameter servers as Diameter AAA server groups that consist of a primary and secondary server.

To define a Diameter AAA server group, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa new-model`	Enables AAA.

	Command	Purpose
Step 2	`Router(config)# aaa group server diameter group-name`	Groups different Diameter server hosts into distinct lists and methods. Configuring AAA server groups allows different servers to be used for each element of AAA. It also defines a redundant set of servers for each element.
Step 3	`Router(config-sg-diameter)# server name auth-port 1645 acct-port 1646`	Configures the name of the Diameter server for the group server. The name specified for this command should match the name of a Diameter peer defined using the **diameter peer** command. **Note** The port numbers 1645 and 1646 are defaults for authorization and accounting, respectively. Explicit port numbers are required only if non-default ports are used.

Defining an Authorization Method List for Prepaid Subscribers

To apply parameters that restrict access to a network for prepaid subscribers, use the following command in global configuration mode:

Command	Purpose
`Router(config)# aaa authorization prepaid method_list group server_group [group server_group]`	Defines an authorization method list for prepaid subscribers and defines the Diameter AAA groups to send records.

Configuring Diameter Protocol Parameters Globally

The GGSN uses global Diameter protocol parameters if you have not defined Diameter parameters at the Diameter peer level.

To configure global Diameter parameters, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# diameter timer {connection | transaction | watchdog} value`	Configures Diameter base protocol timers to use if none have been configured at the Diameter peer level. The valid range, in seconds, is 0 to 1000. The default is 30. • **connection**—Maximum amount of time the GGSN attempts to reconnect to a Diameter peer after being disconnected due to a transport failure. A value of 0 configures the GGSN to not try to reconnect. • **transaction**—Maximum amount of time the GGSN waits for a Diameter peer response before trying another peer. • **watchdog**—Maximum amount of time the GGSN waits for a Diameter peer response to a watchdog packet. When the watchdog timer expires, a DWR is sent to the Diameter peer and the watchdog timer is reset. If a DWA is not received before the next expiration of the watchdog timer, a transport failure to the Diameter peer has occurred. When configuring timers, the value for the transaction timers, should be larger than the value for the TX timer, and, on the SGSN, the values configured for the number GTP N3 requests and T3 retransmissions must be larger than the sum of all possible server timers (RADIUS, DCCA, and Cisco CSG2). Specifically, the SGSN N3*T3 must be greater than 2 x RADIUS timeout + *N* x DCCA timeout + Cisco CSG2 timeout where: • 2 is for both authentication and accounting. • *N* is for the number of Diameter servers configured in the server group.
Step 2	`Router(config)# diameter redundancy`	Enables the Diameter node to be a Cisco IOS Redundancy Facility (RF) client and track session states. The Diameter base does not initiate a connection to a Diameter peer that is in standby mode. Upon a standby-to-active mode transition, a connection to the newly active peer is established. **Note** This command is required for Service-aware PDP session redundancy. For more information about service-aware PDP session redundancy, see the "GTP-Session Redundancy for Service-Aware PDPs Overview" section on page 8-35.
Step 3	`Router(config)# diameter origin realm string`	Configures the realm of origin (part of the domain "@*realm*") in which this Diameter node is located. Origin realm information is sent in requests to a Diameter peer.
Step 4	`Router(config)# diameter origin host string`	Configures the Fully Qualified Domain Name (FQDN) of the host of this Diameter node. The origin host information is sent in requests to a Diameter peer.

	Command	Purpose
Step 5	`Router(config)# diameter vendor support {Cisco | 3gpp | Vodafone}`	Configures this Diameter node to advertise the vendor AVPs it supports in capability exchange messages with Diameter peers. Multiple instances of this command can be configured if the vendor IDs differ.

Monitoring and Maintaining the Diameter Base

To monitor and maintain Diameter peer configurations, use the following command in privileged EXEC mode.

Command	Purpose
`Router# show diameter peer`	Displays Diameter peer-related information.

Configuring the DCCA Client Process on the GGSN

The GGSN functions as a DCCA client when interacting with the DCCA server to obtain and request quota. As a DCCA client, the GGSN sends CCR messages to and receives CCAs from the DCCA server for credit control sessions (one credit control session per PDP session). In addition, the defaults you configure in the DCCA client profile dictate how the GGSN handles credit control sessions if a server switchover should occur and no instructions are sent by the server.

Failure Handling Defaults on the DCCA Client

The following two AVPs determine how the credit-control (CC) sessions are handled if a switchover occurs:

- CC-Session-Failover AVP—Indicates that a CC session should fail over to the alternate Diameter server. You set this AVP by using the **session-failover** command in DCCA client profile configuration mode.
- Credit-Control-Failure-Handling (CCFH) AVP—Determines how the GGSN behaves if a failure does occur. You set this AVP by using the **ccfh** command in DCCA client profile configuration mode.

You can configure defaults for these AVPs in the DCCA client profile for failure handling, however, the values received from the DCCA server override the defaults you configure on the GGSN.

The CCFH AVP determines the action the DCCA client takes on a session when the following fault conditions occur:

- Tx timeout expires.
- CCA message containing protocol error (Result-Code 3xxx) is received.
- CCA fails (for example, a CCA with a permanent failure notification [Result-Code 5xxx]) is received.
- Failure-to-send condition exists. (The DCCA client is not able to communicate with the desired destination.)
- An invalid answer is received.

To configure a DCCA client profile, in which you configure the characteristics of a DCCA client process, and reference to from the charging profile, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs dcca profile name`	Defines the DCCA client process on the GGSN and enters DCCA client profile configuration mode.
Step 2	`Router(config-dcca-profile)# authorization method_list_name`	Defines the method list that is used to specify the Diameter AAA server groups.
Step 3	`Router(config-dcca-profile)# tx-timeout seconds`	Configures a TX timeout value, in seconds, that the DCCA client uses to monitor the communication of CCRs with a Diameter server. The valid range is from 1 to 1000 seconds. The default is 10. When configuring timers, the value for the transaction timer, should be larger than the TX-timeout value, and, on the SGSN, the values configured for the number GTP N3 requests and T3 retransmissions must be larger than the sum of all possible server timers (RADIUS, DCCA, and Cisco CSG2). Specifically, the SGSN N3*T3 must be greater than 2 x RADIUS timeout + *N* x DCCA timeout + Cisco CSG2 timeout where: • 2 is for both authentication and accounting. • *N* is for the number of Diameter servers configured in the server group.
Step 4	`Router(config-dcca-profile)# ccfh {continue | terminate | retry_terminate}`	Configures the default Credit Control Failure Handling (CCFH) action to take on PDP contexts when a fault condition occurs. • **continue**—Allows the PDP context and user traffic for the relevant category or categories to continue, regardless of the interruption. Quota management of other categories is not affected. • **terminate**—Terminates the PDP context and the CC session. • **retry_terminate**—Allows the PDP context and user traffic for the relevant category or categories to continue. Hard-coded quota (1 GB) is passed to the CSG2 when the first DCCA server is unavailable. The DCCA client retries to send the CRR to an alternate server and if a failure-to-send condition occurs with the alternate server, the PDP context is terminated. The default is to terminate. A value from the DCCA server in a CCA overrides this default.

	Command	Purpose
Step 5	`Router(config-dcca-profile)# session-failover`	Specifies that a session should switchover to the alternate DCCA server Configures Credit Control Session Failover (CCSF) AVP support when a CCA message from a DCCA server does not contain a value for the CCSF AVP. By default, session switchover is not supported.
Step 6	`Router(config-dcca-profile)# destination-realm` *string*	Specifies the destination realm to be sent in CCR initial requests to the DCCA server. For subsequent CCRs, the Origin-Realm AVP received in the last CCA is used as the Destination-Realm.
Step 7	`Router(config-dcca-profile)# trigger {plmn-change | qos-change | rat-change | sgsn-change | user-loc-info-change}`	Configures a change that when it occurs, triggers the GGSN (functioning as a DCCA client) to request quota-reauthorization and generate an eG-CDR. • **plmn-id**—PLMN ID change triggers a quota reauthorization request. • **qos-change**—QoS change triggers a quota reauthorization request. • **rat**—RAT change triggers a quota reauthorization request. The RAT indicates whether the SGSN serves the user equipment (UE) UMTS or GSM/EDGE RAN (GERAN). • **sgsn-change**—SGSN change triggers a quota reauthorization request. • **user-loc-info-change**—User location change triggers a quota-reauthorization request. Modifying this command does not affect existing PDP contexts using a DCCA client profile. The **plmn-change**, **rat-change**, and **user-loc-info-change** keyword options require that the GGSN is configured to include these fields in the service-record IE in CDRs using the **gprs charging service record include** command. When configuring triggers: • This command is supported by the generic DCCA client and 3GPP Gy-DCCA only. • Explicitly enable all triggers for both prepaid and postpaid users. • Configured prepaid triggers apply to all of the services that flow through the PDP context. The triggers received for a given service from the OCS server take precedence over the ones configure using the **trigger** command.

Enabling Support for Vendor-Specific AVPs in DCCA Messages

The Cisco GGSN supports the following DCCA implementations:

- VF_CLCI (Vodafone)
- 3GPP Gy-compliant (3GPP)

Note With Cisco GGSN Release 9.0 and later, neither of these implemenations are supported by default. A DCCA implementation must be explicitly enabled using the **gprs dcca 3gpp** command or the **gprs dcca clci** command.

The Gy-compliant implementation supports some additional 3GPP Vendor Specific Attributes (VSAs) in addition to the standard DCCA attributes. The VF_CLCI compliant implementation supports Vodafone specific VSAs, 3GPP VSAs where necessary, and the standard DCCA attributes.

The Cisco GGSN advertises the support of only DCCA application (Auth-Application-Id of 4) in CER messages. In addition, it advertises the support of the following Vendor Ids (for recognizing the vendor specific AVPs).

- Cisco (vendor id = 9)
- 3GPP (vendor id = 10415)
- Vodafone (vendor id = 12645)

To enable the Cisco GGSN to send 3GPP VSAs in DCCA messages to the DCCA server, complete the following task while in global configuration mode.

Command	Purpose
`Router(config)# gprs dcca 3gpp`	Configures the GGSN to send 3GPP VSAs in DCCA messages to the server.

To enable the GGSN to send Vodafone VSAs in DCCA messages to the DCCA server, in addition to the standard DCCA attributes and 3GPP VSAs, complete the following task while in global configuration mode.

Command	Purpose
`Router(config)# gprs dcca clci`	Configures the GGSN to send Vodafone vendor-specific AVPs in DCCA messages to the server.

For a list of supported AVPs in respect to the Gy-based and VF-CLCI, refer to the *Diameter Credit Control Application on the Cisco GGSN* technical whitepaper.

Configuring the Service Aware Billing Parameters in Charging Profiles

The GGSN supports up to 256 charging profiles, numbered 0 to 255. Profile 0 is a set profile that always exists on the GGSN. It is the global default charging profile. You do not create profile 0, however, you can modify it using the charging-related global configuration commands. Profiles 1 to 255 are user-defined and customized using the Cisco GGSN charging profile configuration commands.

To support service-aware billing, you can configure a charging profile to allow eG-CDRs and suppress G-CDRs for all or only online charging.

You can also configure the following service-aware billing characteristics in a charging profile:

- Default rulebase-ID to apply to a user
- Default charging type (to be used primarily for a prepaid or postpaid subscriber)
- DCCA servers to contact for quota requests (presence indicates online charging)

To configure service-aware billing characteristics in a charging profile, complete the tasks in the following sections:

- Specifying a Default Rulebase ID, page 8-25
- Specifying a DCCA Profile for Online Billing, page 8-26
- Suppressing CDRs for Prepaid Subscribers, page 8-27
- Configuring Trigger Conditions for Postpaid Subscribers, page 8-27

Specifying a Default Rulebase ID

In a service-aware implementation with Diameter/DCCA (see the "Implementing Service-Aware Billing with Diameter/DCCA Support" section on page 8-12), rulebases contain the rules for defining categories of traffic; categories on which decisions such as whether to allow or disallow traffic, and how to measure traffic, are based. The GGSN maps Diameter rulebase IDs to Cisco CSG2 billing plans.

To configure a default rulebase ID to apply to PDP contexts using a particular charging profile, use the following command in charging profile configuration mode:

Command	Purpose
`Router(ch-prof-conf)# content rulebase id`	Defines a default rulebase ID to apply to PDP contexts using this charging profile.

Note The rulebase value presented in a RADIUS Access Accept message overrides the default rulebase ID configured in a charging profile. A rulebase ID received in a CCA initial message from a DCCA server overrides the rulebase ID received from the RADIUS server and the default rulebase ID configured in a charging profile.

For Gy:DCCA prepaid solution, the Rulebase ID cannot be received in a DCCA and the Rulebase ID does not apply to the standalone prepaid solution.

Specifying a DCCA Profile for Online Billing

When the primary PDP context is created, the charging profile is selected.

If you define a DCCA profile in the charging profile, online billing is indicated for that PDP. Therefore, regardless of whether or not a user is prepaid or postpaid, the GGSN contacts the DCCA server if the **content dcca profile** configuration is present.

Note This charging profile configuration requires that service-aware billing has been implemented with Diameter/DCCA (see "Implementing Service-Aware Billing with Diameter/DCCA Support" section on page 8-12.)

If the user is to be treated as a postpaid subscriber, the DCCA server returns a CAA with a result-code of CREDIT_CONTROL_NOT_APPLICABLE (4011) and the user is treated as a postpaid subscriber.

If a charging profile does not contain a DCCA profile configuration, users are treated as postpaid (offline billing).

To specify the DCCA client profile to communicate with a DCCA server, use the following command in charging profile configuration mode:

Command	Purpose
`Router(ch-prof-conf)# content dcca profile profile-name [weight max-weight]`	Specifies the profile to communicate with a DCCA server and optionally, assigns a weight to the charging profile for weighted round robin load balancing. A valid weight is a number from 1 to 255. The default is 1.

OCS Load Balancing

In earlier releases of the Cisco GGSN (before Release 10.0), each Cisco SAMI PPC ran a Cisco GGSN instance. The APNs of each GGSN instance were mapped to only one DCCA profile (OCS server), however, the same APN across the Cisco GGSN instances on the Cisco SAMI PPCs could be mapped to different DCCA profiles. Therefore, an APN on a Cisco SAMI hosting six GGSN instances could communicate with one or more OCSs.

With the transition to a Single IP architecture in Cisco GGSN Release 10.0 and later, the separate GGSN instances running on the six Cisco SAMI processors function as a single GGSN instance, therefore, an APN must be able to communicate with multiple DCCA servers.

For efficient OCS utilization, subscribers are load balanced among the OCSs using a weighted round-robin selection of DCCA profiles defined under the charging profile that is applied to an APN. This means that the next DCCA profile defined in a charging profile is used whenever a new primary PDP context uses the charging profile. If you associate a weight to a DCCA profile (using the **weight** keyword option), that profile is used for the corresponding weight before the next DCCA profile is used. The GGSN uses the same OCS/DCCA for the duration of the primary and all secondary PDPs.

Suppressing CDRs for Prepaid Subscribers

In a service-aware implementation with Diameter/DCCA (see "Implementing Service-Aware Billing with Diameter/DCCA Support" section on page 8-12), charging for prepaid subscribers is handled by the DCCA client; therefore, eG-CDRs do not need to be generated for prepaid subscribers.

To configure the GGSN to suppress eG-CDRs for users with an active connection to a DCCA server, use the following command in charging profile configuration mode:

Command	Purpose
`Router(ch-prof-conf)# cdr suppression prepaid`	Specifies that CDRs be suppressed for prepaid subscribers.

Note When G-CDRs suppression is enabled, if a Diameter server error occurs while a session is active, the user is reverted to postpaid status, but CDRs for the PDP context are not generated.

Configuring Trigger Conditions for Postpaid Subscribers

If a user is a prepaid subscriber not using an enhanced quota server interface, all the credit control is performed by the DCCA server. If the user is a postpaid subscriber not using an enhanced quota server interface, and service-aware billing is enabled, the default values configured in a charging profile define the conditions that control how often usages should be reported.

Note Triggers must be explicitly enabled for both prepaid and postpaid subscribers.

To define the trigger conditions in a charging profile for postpaid subscribers, use the following commands in charging profile configuration mode:

	Command	Purpose
Step 1	`Router(ch-prof-conf)# content postpaid {qos-change | sgsn-change | plmn-change | rat-change}`	Configures the condition that, when it occurs, causes the GGSN to request quota reauthorization for a PDP context. • **qos-change**—Quality of Service (QoS) change triggers a quota reauthorization request. • **sgsn-change**—SGSN change triggers a quota reauthorization request. • **plmn-change**—Public land mobile network (PLMN) change triggers a quota reauthorization request. • **rat-change**—Radio access technology (RAT) change triggers a quota reauthorization request. **Note** The **plmn-change** and **rat-change** keyword options require that the GGSN is configured to include the RAT and/or PLMN ID fields in the service-record IE in CDRs using the **gprs charging service record include** command. **Note** Explicitly enable triggers for both prepaid and postpaid subscribers.
Step 2	`Router(ch-prof-conf)# content postpaid time value`	Specifies the time duration limit, in seconds, that causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context when exceeded. The valid value is between 300 and 4294967295 seconds. The default is 1048576.
Step 1	`Router(ch-prof-conf)# content postpaid validity seconds`	Specifies the amount of time, in seconds, that quota granted for a postpaid subscriber is valid. The valid range is from 900 to 4294967295 seconds. The default is no validity timer is configured.
Step 2	`Router(ch-prof-conf)# content postpaid volume value`	Specifies the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR. The valid value is between 1 and 4294967295. The default is 1,048,576 bytes (1 MB).

Implementing Service-Aware Billing with OCS Address Selection Support

As an alternative to the GGSN with DCCA online charging solution, you can configure the GGSN to support OCS address selection. OCS address selection enables online credit control for prepaid subscribers to be provided by an external OCS to which the Cisco CSG2 has a direct GTP' interface. When you configure the GGSN to support OCS address selection, the GGSN functions as a quota server for postpaid subscribers only. The GGSN does not generate enhanced G-CDRs (eG-CDRs) for prepaid subscribers.

By default, the GGSN sends its IP address in Accounting-Start messages to the Cisco CSG2 (functioning as a RADIUS proxy) to establish itself as the quota server for postpaid and prepaid subscribers. When OCS address selection support is configured, if the IP address of an OCS is returned in the "csg:quota_server" attribute in an Access-Accept message from the AAA server, the GGSN forwards that address in the same attribute in an Accounting-Start message to the Cisco CSG2. This notifies the Cisco CSG2 to use the external OCS as the quota server for this PDP context. In a service-aware GGSN implementation using OCS address selection, the GGSN functions as the quota server for postpaid subscribers only.

Service-Aware Billing with OCS Address Selection Data Flows

The following is a high-level overview of the flow of traffic during the creation of a PDP context for a prepaid subscriber in an enhanced service-aware billing implementation using OCS address selection.

1. SGSN sends a Create PDP Context request to the service-aware GGSN.
2. GGSN sends an Access-Request message to the RADIUS endpoint (server or the Cisco CSG2 configured as a RADIUS proxy).
3. RADIUS endpoint determines if the user is prepaid, and if so, responds to the Access-Request message with an Access-Accept message that includes the "csg:quota_server" attribute containing the IP address and port of an external OCS.

4. If the APN is configured as service-aware, and the GGSN is configured to generate eG-CDRs, the GGSN receives the Access-Accept from the RADIUS endpoint, and because the "csg_quota_server" attribute is present and includes the IP address of an OCS, the GGSN determines that the user is a prepaid subscriber, and returns an Accounting-Start request that includes the following attributes:
   - csg:billing_plan
   - csg:quota_server attribute—The "csg:quota_server" attribute contains the OCS IP address and port to the Cisco CSG2. If it does not, the GGSN forwards its own IP address in the "csg:quota_server" field.)
   - csg:eggsn_qs—IP address and port number of the enhanced quota server interface.
   - csg:eggsn_qs_mode—Indicates whether the enhanced quota server interface is enabled to exchange service control messages with the CSG2.
5. Upon receiving the Accounting-Start Request, the RADIUS endpoint performs the following:
   a. Creates a Cisco CSG2 User Table entry.
   b. Identifies that the GGSN generates the eG-CDRs, and disables service level CDR generation for the user.
   c. Identifies that the user is a prepaid user based on the billing plan received.
   d. Enables the quota server message exchange with the specified OCS address.
   e. Enables service control message exchange with the GGSN.
   f. Sends an Accounting-Start Response to the GGSN.
6. GGSN sends a Create PDP Context response to the SGSN, and the context is established.
7. When trigger conditions occur, Service Control Requests (SCRs) and Service Control Usage (SCU) messages are exchanged between the GGSN and CSG2 to add service containers to eG-CDRs, or close eG-CDRs.
8. GGSN generates eG-CDRs and sends them to the charging gateway.

Note When an external OCS is used as the quota server for prepaid subscribers, the GGSN receives service-level usage reports from the Cisco CSG2 for postpaid subscribers and generates eG-CDRs accordingly. The GGSN does not generate eG-CDRs for prepaid subscribers unless an enhanced quota interface has been configured as described in "Configuring the Quota Server Interface on the GGSN" section on page 8-7.

OCS address selection support on the GGSN requires that the following conditions are met:

- Support for service-aware billing is enabled globally and at the APN level (see the "Enabling Support for Service-Aware Billing" section on page 8-3).
- Wait accounting is enabled (using the "Configuring Wait Accounting" section on page 8-4).
- GGSN is configured to communicate with the Cisco CSG2 (see the "Configuring Quota Server Support on the Cisco GGSN" section on page 8-5).
- The GGSN is configured to generate eG-CDRs (see the "Configuring the GGSN to Generate Enhanced G-CDRs" section on page 8-4).
- The correct configuration exists on the AAA server.

To enable OCS address selection support on the GGSN, use the following command in global configuration mode:

	Command	Purpose
Step 1	`Router(conf)# gprs radius attribute quota-server ocs-address`	Configures the GGSN to send the OCS IP address received in an Access-Accept response from a RADIUS server in the csg:quota server attribute in Accounting-Start messages to the Cisco CSG2.

Enabling PCC under an APN

The Gx interface is a reference point between the Policy and Charging Rules Function (PCRF) and the Policy and Charging Enforcement Function (PCEF). It is used for provisioning and removal of Policy and Charging Control (PCC) files from PCRF to PCEF.

When a Create PDP Context request is received from an SGSN on a PCC-enabled APN:

1. After authentication, the GGSN sends an Accounting Start messages to the CSG2 that contains the following Cisco AVPs (in addition to the other standard 3GPP attributes):
   - pcc_enabled—Indicates whether a subscriber is a Gx user. If enabled, the CSG2 marks the subscriber as a Gx user and communicates with the PCRF for this subscribers session. (If not enabled, the CSG2 marks the subscriber as a non-Gx subscriber and does not communicate with the PCRF.)
   - coa_flags—Indicates whether the GGSN supports Gx updates via RADIUS CoA messaging. If enabled, the GGSN supports Gx updates via RADIUS CoA messaging. (If not enabled, indicates MS-initiated QoS updates.)
2. If the GGSN is configured to generate eG-CDRs, in the Accounting Start message, the GGSN includes the following additional attributes:
   - csg:eggsn_qs—IP address and port number of the enhanced quota server interface.
   - csg:eggsn_qs_mode—Indicates whether the enhanced quota server interface is enabled to exchange service control messages with the CSG2.
3. Upon receiving the Accounting-Start Request, the CSG2 performs the following:
   a. Creates a Cisco CSG2 User Table entry.
   b. Identifies that it is a Gx user based on the attributes received.
   c. Identifies that GGSN generates the eG-CDRs, and disables service level CDR generation for the user.
   d. Enables the exchange of service control messages with the enhanced quota server interface defined in the “csg:eggsn_qs” attribute in the Accounting Start message.
4. The CSG2 communicates with the PCRF to provision charging rules and the authorized QoS attributes.
5. The CSG2 sends a CoA request to the GGSN that notifies the GGSN of the authorization status and authorized QoS attributes, and sends an Accounting Start response to the GGSN.
6. The Cisco GGSN receives the CoA request, and based on the authorization status, sends the Create PDP Context response to the SGSN and the PDP context is created.

7. When trigger conditions occur, Service Control Requests (SCRs) and Service Control Usage (SCU) messages are exchanged between the GGSN and CSG2 to add service containers to eG-CDRs, and/or close eG-CDRs.
8. The GGSN generates eG-CDRs and sends them to the charging gateway.

Note If an APN is PCC-enabled, configure the GGSN to wait for a RADIUS accounting start response before sending a Create PDP Context response to the SGSN. For information about configuring wait accounting, see the "Configuring Wait Accounting" section on page 8-4.

To configure an APN as a PCC-enabled APN, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# pcc`	Configures the APN as a PCC-enabled APN.

Configuring Standalone GGSN Prepaid Quota Enforcement

You can implement prepaid quota enforcement using a service-aware GGSN, the Cisco GGSN and Cisco CSG2 implemented together to provide enhanced billing services, or you can implement prepaid quota enforcement using a Cisco GGSN operating in standalone mode.

When you implement the prepaid feature using a Cisco GGSN operating in standalone mode, the GGSN monitors data packets on volume basis, time basis, or both, for each prepaid subscriber. If you have configured the GGSN for both volume and time quota, the GGSN inspects both usages, and requests additional quota as soon as either usage meets its threshold or expires.

When configuring standalone GGSN prepaid quota enforcement:

- Support for service-aware billing must be enabled on the GGSN using the **gprs service-aware** command.
- The measurement of time starts as soon as the session is established.
- The GGSN monitors on a per-user basis, not on a per-service basis.
- In a redundant configuration, the active GGSN synchronizes quota allocated information with the standby GGSN when event triggers occur, such as at the time of each quota grant. Periodic synchronization of quota usage information is not performed. To ensure a user is not overcharged, the standby and active GGSNs maintain synchronization of the CC-Request-Number along with each quota grant.
- The GGSN monitors quota on a per-user basis, therefore, when the standalone GGSN requests quota, only one service is expected in the Multiple-Service-Credit-Control [MSCC] AVP. If the CCA contains multiple services, or no service in the MSCC AVP, the CCA is considered an invalid answer, and the CCFH determines the action.
- Only single service is supported. If multiple services are configured, the CCFH determines whether the GGSN rejects the PDP or converts it to postpaid.
- With a dual quota, the Quota Holding Timer (QHT) starts after the Quota Consumption Timer (QCT). Even though the QCT does not apply to volume quota, this behavior is due to time quota. With time quota, the QHT starts after the quota consumption ceases, which occurs after the QCT.
- If a DCCA profile is not configured under the charging profile, the PDP is rejected.

- Once a PDP is converted to postpaid, enhanced G-CDRs are no longer generated, only G-CDRs.
- In a redundant configuration, all timers (QHT, QCT, time threshold, etc.) except for the Quota Validity Timer (QVT) are restarted once the standby GGSN becomes active. The QVT timestamp is synchronized, and when a standby GGSN becomes active, the newly active GGSN waits for the remaining time to elapse instead of restarting the timer.

To configure the GGSN to perform quota enforcement for prepaid subscribers in standalone mode, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs prepaid stand-alone`	Configures the GGSN to perform prepaid quota enforcement in standalone mode.

To configure the maximum limit on the volume/time quota threshold in terms of percentage of the volume/time quota received, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs prepaid quota threshold` *percentage*	Sets the maximum limit on the volume/time quota threshold, as a percentage of the volume/time quota grant received from the DCCA server on the threshold received. The valid value is 0 to 100 percent. The default is 80.

When you configure the prepaid quota threshold, the threshold value used on the GGSN is the lower value between the:

- Threshold value, in percentage, received in a CCA
- Configured percentage of the quota grant

To monitor standalone quota enforcement, use the following commands in privileged EXEC mode:

Command	Purpose
`Router# clear gprs prepaid quota sanity`	Clears sanity statistics of the GPRS quota grant parameters.
`Router# clear gprs prepaid statistics`	Clears GGSN quota-manager statistics.
`Router# show gprs prepaid quota sanity`	Displays sanity statistics of the GPRS quota grant parameters.
`Router# show gprs prepaid statistics`	Displays GGSN quota-manager statistics.

Configuring the Charging Record Type under an APN

With Cisco GGSN Release 9.2, and later, you can configure the charging record type for an APN. This command is supported when one of the following conditions exists:

- You have configured the APN to be service-aware (see the "Enabling Support for Service-Aware Billing" section on page 8-3) or PCC-enabled (see the "Enabling PCC under an APN" section on page 8-31).
- You have configured the quota server interface to support the exchange service control messages (see the "Configuring the Quota Server Interface on the GGSN" section on page 8-7).
- You have configured GPRS Charging Release 7 (see the "Configuring the Charging Release" section on page 7-8).

To configure the charging record type for an APN, use the following command in access-point configuration mode:

Command	Purpose
`Router(access-point-config)# charging record type [gcdr | egcdr | none]`	Configures the charging record type for an APN, where: • **gcdr**—G-CDRs are generated. • **egcdr**—eG-CDRs are generated. • **none**—No records are generated. By default, G-CDR generation is enabled, however, it can be disabled by using the **cdr suppression** command in access-point configuration mode.

You can configure the charging record type in the following modes:

- Global configuration
- Charging profile configuration
- Access-point configuration

When configuring the charging record type at the APN level, note that the charging profile configuration overrides the global configuration, and the APN level configuration overrides the charging profile configuration.

For example, you can enable eG-CDR generation globally by using the **gprs charging cdr-option service-record** command, and then configure the **charging record type gcdr** command under an APN to restrict the user of that APN to generate G-CDRs. The remaining service aware users generates eG-CDRs.

If the charging record type command is not configured at the APN level, the default behavior is based on the existing eG-CDR generation global configuration set by using the **gprs charging cdr-option service-record** command.

GTP-Session Redundancy for Service-Aware PDPs Overview

GTP-Session Redundancy (GTP-SR) ensures that when an active GGSN fails, a standby GGSN has all the necessary information about a PDP context to continue service without interruption. In an enhanced service-aware billing environment, this means service-related information must also be synchronized from the active to standby service-aware GGSN. Therefore, with GGSN Release 5.2 and later, service-aware data necessary to establish charging for service-aware PDP sessions is synchronized with the standby GGSN.

The service-aware data synchronized with the standby GGSN includes the following:

- Per-PDP context services—Rulebase ID and DCCA failure handling settings (CCSF and CCSH AVPs).
- Per-category information—Category ID, Cisco CSG2 session, and category state and event triggers. Many category states are intermediate states; therefore, they are not synchronized to the standby service-aware GGSN. The following category states are synchronized: “blacklist,” “idle,” and “authorized.”

  All event triggers are recorded. At the end of the processing of an event on the active GGSN, the clearing of the event’s trigger is synchronized to the standby GGSN. If a switchover occurs, if an event trigger is found present on a category, the newly active GGSN re-initiates the event.
- Path states—The quota server process on the active GGSN synchronizes the state of the path to a Cisco CSG2 to the quota server process on the standby GGSN. The path echo timer on the standby quota server is not started unless the standby quota server becomes active. Path sequence numbers are not synchronized. After a switchover occurs, the newly active quota server starts from 0.

Note Category usage data is not synchronized from an active GGSN to the standby GGSN. This prevents over-reporting of usage if a switchover occurs.

GTP-SR for Service-Aware PDP Sessions Guidelines

In addition to the prerequisites listed in Chapter 6, “Configuring GGSN GTP Session Redundancy,” to achieve session redundancy for service-aware PDP sessions, ensure that the following configurations exist on the redundantly configured service-aware GGSN:

- GTP-SR is enabled on the GGSN using the **gprs redundancy** command in global configuration mode. Also, if the GGSN is functioning as a Diameter node, ensure that it is enabled to track session states by using the **diameter redundancy** command in global configuration mode. See the “Configuring the Diameter Base” section on page 8-16 for information on configuring Diameter redundancy.
- The quota server process is configured the same on both the active GGSN and the standby GGSN. Specifically, on each active/standby pair, the quota server address is the same. To ensure that the Cisco CSG2 only talks to the active quota server process, configure it to always route messages for the quota server through the virtual HSRP address for the Gi interface. In reverse, the virtual Cisco CSG2 address is used by the GGSN to deliver messages to the active Cisco CSG2 of a redundant pair. See the “Configuring a Cisco CSG2 Server Group” section on page 8-6 for more information about configuring a virtual Cisco CSG2 address.
- If using Diameter, configure a DCCA client source address on both the active GGSN and the standby GGSN. The DCCA client source address is the local address used in the TCP connection to the DCCA server. We recommend that you use a logical interface that is routable via a virtual HRSP address between the active GGSN and the standby GGSN.

For information on configuring Cisco IOS HRSP, see *Configuring the Hot Standby Router Protocol* section of the *Cisco IOS IP Configuration Guide, Release 12.3*. For detailed information on GTP-SR, see Chapter 6, "Configuring GGSN GTP Session Redundancy."

For information about fault-tolerance on the Cisco CSG2, see *Cisco Content Services Gateway - 2nd Generation Release 3.5 Installation and Configuration Guide*.

Configuring Per-Service Local Sequence Number Synchronization

The charging gateway uses the per service local sequence number to detect duplicate service containers associated with a PDP context.

To minimize the amount of data being synchronized to the standby GGSN, the per service local sequence number is not synchronized each time an eG-CDR is closed. Instead, the current value of the local sequence number and the local sequence number last synchronized for a PDP context is checked, and if the difference is more than the configured window size, the current local sequence number is synchronized with the standby GGSN. When a standby GGSN becomes the active GGSN, it starts from the last value synchronized, plus the window size.

To configure the window size that determines when the per service local sequence number is synchronized with the standby GGSN, use the following command in global configuration mode:

Command	Purpose
`Router# gprs redundancy charging sync-window svc-seqnum size`	Configures the window size that determines when the per service local sequence number is synchronized with the standby GGSN. The valid value is a number between 1 and 200. The default is 50.

Configuring Activity-Based Time Billing for Prepaid Subscribers

Cisco GGSN Release 10.0 supports activity-based time billing is an enhancement to the standard duration-based billing.

Activity-based billing, as defined by 3GPP standards, bills subscribers for only the time they are active on the network instead of the entire time they are logged on to the network. This feature enables you to eliminate charging for periods of inactivity between packets.

To support activity-based time billing, in an eGGSN implementation, the Cisco GGSN receives the quota consumption time (QCT) AVP and the quota holding time (QHT) AVP in the CCA for each of the services (i.e. MSCC) from the OCS. In a Service Authorization Response, a Service Reauthorization Response, or a Quota Push message, the Cisco GGSN forwards the QCT and QHT values to the Cisco CSG2.

Note The QCT and QHT values sent from the OCS, and forwarded to the Cisco CSG2 by the Cisco GGSN, take precedence over the values configured on the Cisco CSG2. If the GGSN does not receive the QCT or QHT AVP from the OCS, the Cisco CSG2 uses locally configured QCT and QHT values.

The QCT is the maximum time a user can be charged during periods of inactivity. The QHT corresponds to the service idle timeout configured on the Cisco CSG2. The Cisco GGSN quota server QHT overrides the service idle timeout configured on the Cisco CSG2, as well as any prior quota server QHTs.

For information about activity-based time billing on the Cisco CSG2, see *Cisco Content Services Gateway - 2nd Generation Release 4 Installation and Configuration Guide, Cisco IOS Release 12.4(24)MD*.

There are no new or modified Cisco GGSN commands for Activity-Based Time Billing support.

Configuring HTTP Redirection

The Cisco GGSN supports Final Unit Indication (FUI) HTTP redirection and termination (introduced in Cisco IOS Release 12.4(24)YE) and RADIUS controlled HTTP redirection (introduced in Cisco IOS Release 12.4(24)YE3). Both methods of redirection can be configured under an APN at the same time.

This section contains information on the following:

- Configuring FUI-Based HTTP Redirection, page 8-37
- Configuring RADIUS Controlled HTTP Redirection, page 8-40

Configuring FUI-Based HTTP Redirection

With Cisco GGSN Release 10.0, Cisco IOS 12.4(24) YE and later, an OCS can ask the GGSN to take final action when the account of a subscriber no longer has an adequate number of credits, and the last packet cannot go through because the quota has been exhausted. When this condition occurs, the OCS sends a Final Unit Indication (FUI) attribute value pair (AVP) in a CCA.

The OCS sends the FUI AVP in a CCA at the service (Multiple-Service-Credit-Control[MSCC]) level. The FUI sent by the OCS contains a grant of quota that represents the final units of quota for a service, and contains an action that the GGSN must take once the subscriber to that service uses the final units of quota.

Note The Cisco GGSN supports the FUI in Standalone Mode as well as in an eGGSN implementation. In an eGGSN implementation, the Cisco GGSN uses the Cisco CSG2 as an enforcement point to implement the FUI action. The Cisco GGSN sends the FUI TLV in a Service Authorization Responses or Quota Push Messages to the Cisco CSG2 to communicate the action for the Cisco CSG2 to take.

The possible FUI actions supported by the Cisco GGSN are TERMINATE or REDIRECT final actions.

FUI REDIRECT

Note FUI redirect filters are applied to all uplink and downlink traffic. The filter names can come from the OCS, or you can configure FUI filters under an APN using the **redirect http rule** command in access-point configuration mode.

- If the CCA does not contain a redirect server address, the Cisco GGSN ignores the message and allows service to continue.
- If the CCA contains a redirect server address and granted service units (GSU) with final units for the service, the Cisco GGSN performs the following actions, depending on whether it is operating in standalone mode or in an eGGSN implementation:
  - In standalone mode, after the final units of quota are consumed, the Cisco GGSN returns the quota to the OCS, indicating that the redirect action has started and the subscriber should be redirected to the redirect server. (The OCS provided redirection takes precedence over any existing redirect configuration.) Downlink packets that are allowed by weight 0 filter continue to flow to the subscriber. Once the subscriber replenishes their account, the OCS allows the subscriber to continue the service by reauthorizing the service. After a successful reauthorization, the original uplink user plane is restored. If the subscriber does not replenish the account with more quota, the service is terminated after the validity time.
  - In an eGGSN implementation, in response to a service authorization request, the FUI is sent to the Cisco CSG2 with the redirection action set. After the final units of quota are consumed, the Cisco CSG2 returns the quota to the GGSN (GGSN returns to OCS) indicating that the redirect action has started, and redirect the subscriber to the redirect server. If the subscriber does not replenish the account with more quota, the service might be terminated by indication from the OCS (CCA after the validity time).
  - In an eGGSN implementation, the Cisco GGSN sends the GSU, FUI with redirection action set, and a redirect server address to the Cisco CSG2. When the final quota is spent, the Cisco CSG2 returns the quota to the GGSN (GGSN returns to the OCS) indicating the service is being redirected. If the subscriber does not replenish their account with more quota, the service might be terminated by the OCS (CCA after the validity time).

    Note If the GGSN does not provide a dynamic URL, the Cisco CSG2 uses the redirect URL configured on the **ip csg redirect** command in global configuration mode.

    For more information about the **ip csg redirect** command, see *Cisco Content Services Gateway - 2nd Generation Release 4 Installation and Configuration Guide, Cisco IOS Release 12.4(24)MD*.
- If a CCA does not contain GSU, in both standalone mode and in an eGGSN implementation, the service is immediately redirected, and after redirection, if the subscriber does not replenish the account in a timely manner, the PDP is terminated.

FUI-Action TERMINATE

- If the group AVP in the CCA has any other AVP in it, such as a Redirect-Server_address, the Cisco GGSN terminates the category as follows:
  - In standalone mode, once the final units for the service are consumed, the Cisco GGSN sends the CCR(final) to the OCS and the PDP context is deleted.
  - In an eGGSN implementation, in response to a service authorization request, the FUI TLV is sent to the Cisco CSG2 with the termination action set. Once the final units for the service are consumed, the Cisco CSG2 sends a Service STOP to the Cisco GGSN, and the Cisco GGSN sends a CCR(update) or CCR(final) and terminates the service. If it is the last service, the PDP context is deleted.
- If the CCA also contains the GSU AVP with final units for the service, the following actions occur:
  - In standalone mode, the Cisco GGSN sends the CCR(final) to the OCS and the PDP context is deleted after the final units are consumed.
  - In an eGGSN implementation, the Cisco GGSN sends a CCR(update) or CCR(final) and terminates the service. If it is the final service, the PDP context is deleted.

Note In an eGGSN implementation, if the OCS sends both the FUI-action REDIRECT and FUI-action RESTRICT in the same CCA, the GGSN forwards both actions and their associated TLVs to the Cisco CSG2. When both are received, the Cisco CSG2 ignores the FUI-action RESTRICT and processes the FUI-action REDIRECT.

Configuring a Default FUI Redirection Rule and Local Filters

Note The Cisco GGSN supports the FUI redirection filter configuration when in standalone prepaid mode.

The OCS should return Filter IDs in the FUI group TLV. If the OCS server does not include the Filter IDs in the FUI TLV, the Cisco GGSN FUI-based HTTP redirection configures the GGSN to look for a preconfigured ACL for the FUI REDIRECT action. If an APN does not have a redirect filter defined, and the OCS server does not include a filter ID, all packets are dropped and redirection does not occur.

To configure a rule and FUI filter to apply under an APN if a filter ID is not received in the FUI TLV from the OCS, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# redirect http rule` *acl-number* [**filter-id** *acl-number-in acl-number-out*]	Configures a default FUI rule under an APN if a filter ID is not received in the FUL TLV from the OCS. Optionally, specify the **filter-id** keyword option to apply an FUI redirection filter to a packet before it is dropped to verify if the packet is TCP, and if so, initiate HTTP redirection.

Example 1

In the following Filter ID/ACL configuration example, the redirect server cluster is allowed 172.168.0.1 - 172.168.0.6 for both uplink and downlink traffic.

```
ip access-list extended redirect-example-out
  permit tcp any 172.168.0.1 0.0.0.248 eq www
  permit icmp any any
  permit udp any any eq domain

ip access-list extended redirect-example-in
  permit tcp 172.168.0.1 0.0.0.248 any eq www
  permit icmp any any
  permit udp any any eq domain
```

Example 2

The following ACL is used when a packet is about to be dropped to verify if the packet is TCP. If it is TCP ACK, the GGSN initiates an HTTP redirection from the GGSN.

```
access-list 100 permit tcp any any eq www
```

Example 3: Configuring a Default FUI Filter at an APN

The following example applies a FUI-based redirect HTTP filter to an APN:

```
GGSN(config-access-point)# redirect http rule 100 filter-id redirect-example-in
redirect-example-out
```

Configuring RADIUS Controlled HTTP Redirection

With Cisco GGSN Release 10.1, Cisco IOS Release 12.4(24)YE3 and later, the RADIUS Controlled HTTP Redirection feature enables the Cisco GGSN to redirect the HTTP traffic of subscribers to an Advice-of-Charge (AoC) page that notifies them of new tariff changes when they are roaming in a foreign PLMN.

Cisco GGSN Release 10.1 supports the following new AVPs in RADIUS Access-Accept messages to implement the RADIUS Controlled Redirection feature:

- Address-Type (IP or URL)
- Redirect-Address (IP or URL)
- Filter-ID (preventing access for both downlink (DL) and uplink (UL) traffic to other L3/L4 destinations)
- Redirect-Time (the time after which the redirection or filter-ids are removed)

During the create PDP context request process, AAA sends, at minimum, the mandatory attributes (Address-Type and the Redirect-Address) to the GGSN in an Access-Accept message. When the Cisco GGSN receives these attributes, it applies the RADIUS controlled redirection attributes and sends a create PDP response to the SGSN.

Note The Cisco GGSN downloads five attributes from AAA. These attributes include the two mandatory attributes (Address-type and Redirect-Address). The other attributes (DL and UL Filter-IDs and Redirect-Time) are optional from AAA. If these options are not downoaded from AAA, an operator must configure them under the APN for RADIUS Controlled HTTP Redirection to work.

Note In an eGGSN implementation, the wait accounting feature must be enabled using the **gprs gtp response-message wait-accounting** global configuration command.

With RADIUS-controlled HTTP redirection, note the following:

- If DL/UL filters or values for the redirect interval are not downloaded from AAA, then the values configured under APN using the **redirect radius-controlled** command are used. Also, the **redirect radius-controlled rule** *acl-number* command configures the ACL to use when a packet is about to be dropped, to verify if the packet is TCP, and if TCP ACK, to punt the packet to the process path and initiated an HTTP redirect packet from the GGSN.

  Note The **redirect radius-controlled rule** *acl-number* command is mandatory, regardless of whether the RADIUS Controlled Redirection attributes are downloaded from AAA or are configured locally.

- If the redirect server type and redirect server address are not found in the Access-Accept message from AAA, the GGSN processes the create PDP context request as a normal subscriber who does not need RADIUS controlled HTTP redirection.
- The RADIUS configuration takes precedence over the APN configuration.
- If a redirect interval (Redirect-Time AVP) is not found in the Access-Accept message or a value is not configured locally, the Cisco GGSN uses a default interval of 60 seconds.
- Both FUI-based and RADIUS-controlled redirection can exist at the same time under an APN.

Configuring a Default RADIUS Controlled Redirection Rule and Local Filters

The Cisco GGSN should receive two Filter-IDs from AAA and a Redirect-Time in an Access-Accept message. If the Access-Accept message does not include the filter-ids and redirect time, the GGSN uses values that are configured locally.

Note Values received from AAA take precedence over the locally configured values.

To configure a default RADIUS controlled redirection rule, and local filter IDs and a redirect time, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# redirect radius-controlled rule` *acl-number* `[filter-id` *acl-number-in acl-number-out*`] [interval` *seconds*`]`	Configures a default RADIUS-controlled rule under APN, where the required *acl-number* variable is the number of the access control list (ACL) to apply. Optionally, • Specify the **filter-id** keyword option to specify the filter to apply to a packet to check the weight of traffic destined for the redirect server IP or URL. • Specify the **interval** keyword option to specify, in seconds, the time after which the redirection or filter-ids are removed. The default value is 60.

Note The bare minimum configuration to enable RADIUS-Controlled HTTP Redirection is **redirect radius-controlled rule** *acl-rule*. This configuration will define an ACL rule and a default interval of 60 seconds.

Example 1

In the following Filter ID/ACL configuration example, the redirect server cluster is allowed 172.168.0.1 - 172.168.0.6 for uplink TCP traffic and permit any TCP traffic for downstream:

```
ip access-list extended redirect-example-out
        permit tcp any 172.168.0.1 0.0.0.248 eq www
        permit icmp any any
        permit udp any any eq domain
ip access-list extended redirect-example-in
        permit tcp any any
        permit icmp any any
        permit udp any any eq domain
```

Example 2

The following ACL is used when a packet is about to be dropped to verify if the packet is TCP. If it is TCP ACK, the GGSN initiates an HTTP redirection from the GGSN.

```
access-list 100 permit tcp any any eq www
```

Note The **access-list** command is mandatory, regardless of whether RADIUS controlled redirection attributes are downloaded from AAA or configured locally.

Example 3

The following example applies a RADIUS controlled redirect HTTP filter to an APN:

```
GGSN(config-access-point)# redirect radius-controlled rule 100 filter-id
redirect-example-in redirect-example-out interval 30
```

Verifying the RADIUS Redirection Information

To view the RADIUS controlled redirection related information, use the **show gprs gtp pdp-context** command and specify the **tid** keyword option. The RADIUS controlled redirection information appears in bold.

```
GGSN_Active#show gprs gtp pdp-context tid 2222222222000010
TID MS Addr Source SGSN Addr APN
2222222222000010 172.2.3.4 Static 1.0.0.1 csg.cisco.com

current time :Nov 29 2010 17:57:37
user_name (IMSI): 222222222200000 MS address: 172.2.3.4
MS International PSTN/ISDN Number (MSISDN): 44444444444
sgsn_addr_signal: 1.0.0.1 sgsn_addr_data: 1.0.0.1
control teid local: 0x02100003
control teid remote: 0x10001441
data teid local: 0x02100004
data teid remote: 0x10001442
primary pdp: Y nsapi: 1
signal_sequence: 0 seq_tpdu_up: 9
seq_tpdu_down: 10
upstream_signal_flow: 0 upstream_data_flow: 0
downstream_signal_flow: 0 downstream_data_flow: 0
RAupdate_flow: 0
pdp_create_time: Nov 29 2010 17:55:28
last_access_time: Nov 29 2010 17:57:17
mnrgflag: 0 tos mask map: B8
session timeout: 0
idle timeout: 580

Radius redirection info
----------------------
Radius redirect server: 70.0.0.48
Radius IN filter-id : inacl
Radius OUT filter-id : outacl
Redirection Interval:00:05:00 (300)
Remaining Interval: 169

umts qos_req: 0911012901010111050101
umts qos_neg: 0911012901010111050101
QoS class: conversational
rcv_pkt_count: 10 rcv_byte_count: 1000
send_pkt_count: 10 send_byte_count: 1000
cef_up_pkt: 5 cef_up_byte: 500
cef_down_pkt: 5 cef_down_byte: 500
cef_drop: 0 out-sequence pkt: 0
charging_id: 46514448
visitor: No roamer: Unknown
charging characteristics: 1
charging characteristics received: 0
pdp reference count: 1
primary dns: 0.0.0.0
secondary dns: 0.0.0.0
primary nbns: 0.0.0.0
```

Configuring Cisco CSG2 Load Balancing

With Cisco GGSN Release 10.0 and later, in a service-aware GGSN implementation, the Single IP Cisco GGSN quota server interface can communicate with multiple Cisco CSGs.

To efficiently utilize the Cisco CSGs, subscribers are load balanced among the Cisco CSG2s, and once a Cisco CSG2 has been selected for a particular subscriber, all interfaces communicate with that Cisco CSG2.

Support for Cisco CSG2 load balancing involves the following:

- Support for the configuration of multiple Cisco CSG2 groups per APN.
- Selection of a Cisco CSG2 via dynamic subnet mapping or static subnet mapping.

Note To enable downlink traffic to reach the correct Cisco CSG2, routes need to be present on the supervisor either through static routes or dynamic routes advertised by a Cisco CSG2 via OSPF.

Note The Cisco GGSN gives priority to static mapping configurations over dynamic subnet creation.

Configuring Dynamic Cisco CSG2 Load Balancing

With dynamic load balancing, the subscriber-to-Cisco CSG2 mapping is dynamically determined during the create PDP context process.

The Cisco CSG2 selection is based on the IP address allocated to the subscriber, and the subnet formed by the Cisco GGSN subnet manager under the APN. Once a Cisco CSG2 has been chosen for a subscriber, the same Cisco CSG2 is chosen for the same subnet for different TCOPs and Cisco GGSNs in the same administrative domain.

Note Before configuring a Cisco CSG2 group, ensure that a RADIUS interface for accounting services has been configured for the CSG group using the **aaa-group accounting** command in CSG group configuration mode (see Configuring a Cisco CSG2 Server Group, page 8-6).

To configure a dynamic subnet-to-Cisco CSG2 group mapping, use the following commands in access-point configuration mode:

	Command	Purpose
Step 1	`Router(config-access-point)# aggregate 0.0.0.0 sub-mask`	Configures a default subnet mask for subnet management and enables dynamic subnet creation. **Note** The load balancer function selects a Cisco CSG2 based on the subnet.
Step 2	`Router(config-access-point)# csg-group csg-group-name`	Configures one or more Cisco Content Services Gateway - 2nd Generation (CSG2) group under the APN.

Note The **csg-group** access point configuration command and the **csg group** quota server configuration command are mutually exclusive. You cannot define a CSG group under an APN if one is already configured under the quota server interface.

Configuring Static Cisco CSG2 Mapping

Static load balancing supports an eGGSN implementation for which an external load balancing is being used for RADIUS and data traffic. In this configuration, operators can configure a static subnet-to-Cisco CSG2 mapping under the an APN.

To configure a static subnet-to-Cisco CSG2 group mapping, use the following commands in access-point configuration mode:

	Command	Purpose
Step 1	`Router(config-access-point)# csg-group csg-group-name`	Configures one or more Cisco Content Services Gateway - 2nd Generation (CSG2) group under the APN.
Step 2	`Router(config-access-point)# aggregate subnet-addr subnet-mask csg-group-name`	Configures a static subnet-to-Cisco CSG2 group mapping.

Note The **csg-group** access point configuration command and the **csg group** quota server configuration command are mutually exclusive. You cannot define a CSG group under an APN if one is already configured under the quota server interface.

Reviewing Trigger Conditions for Enhance Quota Server Interface Users

The Cisco GGSN generates eG-CDRs when the following types of trigger conditions occur when the Cisco CSG2 has a direct interface to an OCS, when a subscriber is a Gx user, or when a user is postpaid:

- PDP Context Modification, page 8-46
- Tariff Time Change, page 8-46
- Service Flow Reports, page 8-46
- eG-CDR Closure, page 8-47

Note The following trigger conditions do not require any special configuration on the GGSN. Volume and duration, and service flow triggers must be configured on the Cisco CSG2. For information about configuring the Cisco CSG2, see *Cisco Content Services Gateway 2nd Generation - Release 3.5 Installation and Configuration Guide.*

PDP Context Modification

When one of the following PDP context modification triggers occurs, the GGSN performs the following actions:

- RAT type, PLMN change, or MS time zone change
  - Adds a volume container followed by the list of service containers.
  - Closes the eG-CDR.
  - If a SVC record limit is reached, closes the eG-CDR, opens a partial CDR, and adds the remaining SVC records to the new eG-CDR.
- QoS change or user location change
  - Adds a volume container followed by a list of service containers.
  - If the maximum change condition limit is reached, closes the eG-CDR.
  - If a SVC record limit is reached, closes the eG-CDR, opens a partial CDR, and adds the remaining SVC records to the new eG-CDR.
- SGSN change
  - Adds a volume container followed by a list of service containers.
  - If the maximum SGSN limit is reached, closes the eG-CDR.
  - If the maximum change condition limit is reached, closes the eG-CDR.
  - If there an SVC record limit is reached, closes the eG-CDR, opens a partial CDR, and adds the remaining SVC records to the new eG-CDR.

Tariff Time Change

When a tariff time change occurs, the GGSN performs the following actions:

- Adds a volume container.
- If the maximum change limit is reached, closes the eG-CDR.
- For a prepaid GTP' user, the Cisco CSG2 might send a service usage message and the GGSN would then add it to the eG-CDR.

Service Flow Reports

When the following service flow trigger conditions occur, the GGSN generates service containers for each service:

- Time limit expiration
- Volume limit expiration
- Service flow termination

Volume and duration, and service flow triggers must be configured on the Cisco CSG2. For information about configuring volume and duration triggers, and service flow triggers on the Cisco CSG2, see *Cisco Content Services Gateway 2nd Generation - Release 3.5 Installation and Configuration Guide*.

Additionally, for prepaid GTP' users, the GGSN generates service containers for the following trigger conditions when the same triggers are configured on the Cisco CSG2:

- Time threshold reached
- Volume threshold reached
- Time quota exhausted
- Volume quota exhausted
- Service data flow termination or when service idles out

eG-CDR Closure

When the following eG-CDR closure trigger conditions occur, the GGSN adds the volume containers followed by service containers, except for when CDRs are manually cleared:

- End of PDP context
- Partial record reason
  - Data volume limit
  - Time limit
  - Maximum number of charging condition changes (QoS, tariff time, user-location-info change)
  - Management intervention
  - MS time zone change
  - Inter-PLMN SGSN change
  - RAT change

Configuration Examples

The following is an example of enhanced service-aware billing support configured on the GGSN.

```
Current configuration :3537 bytes
!
! Last configuration change at 15:26:45 UTC Fri Jan 7 2005
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service gprs ggsn
!
hostname sup-samiA
!
boot-start-marker
boot-end-marker
!
enable password abc
!
aaa new-model
!
!
!Configures the CSG2 RADIUS server group
!
aaa group server radius CSG-group
```

```
server 10.10.65.100 auth-port 1812 acct-port 1813
!
!Configures the Diameter server group
!
aaa group server diameter DCCA
server name DCCA
!
!
!Assigns AAA services to the CSG2 RADIUS and Diameter server groups
!
aaa authentication ppp CSG-list group CSG-group
aaa authorization prepaid DCCA group DCCA
aaa authorization network CSG-list group CSG
aaa accounting network CSG-list start-stop group CSG-group
aaa session-id common
ip subnet-zero
!
!
ip cef
!
!
...
!
!
gprs access-point-list gprs
!
...
!
!
!Enables service-aware billing on the GGSN
!
gprs service-aware
!
gprs access-point-list gprs
 access-point 10
  access-point-name cisco.com
  access-mode non-transparent
  aaa-group authentication CSG-list
  aaa-group accounting CSG-list
  gtp response-message wait-accounting
  charging profile any 1 override
  service-aware
  advertise downlink next-hop 10.10.150.2
  !
 access-point 20
  access-point-name yahoo.com
  access-mode non-transparent
  aaa-group authentication CSG
  aaa-group accounting CSG
  gtp response-message wait-accounting
  charging profile any 1 override
  service-aware
  !
 !
!
!Configures a DCCA client profile
!
gprs dcca profile 1
  ccfh continue
  authorization CSG-list
  destination-realm cisco.com
  trigger sgsn-change
  trigger qos-change
!
```

```
gprs charging profile 1
  limit volume 64000
  limit duration 64000
  content rulebase PREPAID
  content dcca profile 1
  content postpaid volume 64000
  content postpaid time 1200
  content postpaid qos-change
  content postpaid sgsn-change
!
!Congigures the quota server
!
ggsn quota-server qs
 interface Loopback2
 csg group csg_1
 !
!
!Configures a CSG2 group
!
ggsn csg-group csg_1
 virtual-address 10.10.65.10
 port 4386
 real-address 10.10.65.2
 !
tftp-server abcbar
!
radius-server host 10.10.65.100 auth-port 1812 acct-port 1813
radius-server host 10.20.154.201 auth-port 1812 acct-port 1813
radius-server key abc
radius-server vsa send accounting
radius-server vsa send accounting 3gpp2
!
!configures Diameter global parameters
!
diameter origin realm corporationA.com
diameter origin host sup-sami42.corporationA.com
diameter vendor supported cisco
!
!configures Diameter peer
!
diameter peer DCCA
 address ipv4 172.18.43.59
 transport tcp port 4100
 timer connection 20
 timer watchdog 25
 destination realm corporationA.com
!
!
...
!
end
```