Cisco ASR 5000 Series IP Services Gateway Administration Guide

Version 12.0

Last updated September 30, 2011

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

Text Part Number: OL-24899-02

Cisco ASR 5000 Series IP Services Gateway Administration Guide

CONTENTS

About this Guide

This document pertains to the features and functionality that run on and/or that are related to the Cisco® ASR 5000 Chassis, formerly the Starent Networks ST40.

Conventions Used

The following tables describe the conventions used throughout this documentation.

Icon	Notice Type	Description
	Information Note	Provides information about important features or instructions.
	Caution	Alerts you of potential damage to a program, device, or system.
	Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.
	Electro-Static Discharge (ESD)	Alerts you to take proper grounding precautions before handling a product.

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`
Text represented as **`commands`**	This typeface represents commands that you enter, for example: **`show ip access-list`** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a **`command`** *`variable`*	This typeface represents a variable that is part of a command, for example: **`show card`** *`slot_number`* slot_number is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**

Command Syntax Conventions	Description
{ **keyword** or *variable* }	Required keywords and variables are surrounded by grouped brackets. Required keywords and variables are those components that are required to be entered as part of the command syntax.
[**keyword** or *variable*]	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by square brackets.
|	With some commands there may be a group of variables from which the user chooses one. These are called alternative variables and are documented by separating each variable with a vertical bar (also known as a pipe filter). Pipe filters can be used in conjunction with required or optional keywords or variables. For example: **{ nonce | timestamp }** OR [**count** *number_of_packets* | **size** *number_of_bytes*]

Contacting Customer Support

Use the information in this section to contact customer support.

For New Customers: Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

For Existing Customers with support contracts through Starent Networks: Refer to the support area of https://support.starentnetworks.com/ for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

Important: For warranty and repair information, please be sure to include the Return Material Authorization (RMA) tracking number on the outside of the package.

Chapter 1
IP Services Gateway Overview

This chapter provides an overview of the IP Services Gateway (IPSG) product.

This chapter covers the following topics:

Introduction

The IP Services Gateway (IPSG) is a stand-alone device capable of providing managed services to IP flows. The IPSG is situated on the network side of legacy, non-service capable GGSNs, PDSNs, HAs, and other subscriber management devices. The IPSG can provide per-subscriber services such as Enhanced Charging Service, Application Detection and Control, and others.

The IPSG allows the carrier to roll out advanced services without requiring a replacement of the HA, PDSN, GGSN, or other access gateways and eliminates the need to add multiple servers to support additional services.

Licensing

IPSG is a licensed product. In order to enable and configure IPSG, one of the following licenses must be installed on the chassis:

- Cisco PID [ASR5K-00-IG01SESS] *IP Service Gateway Base License, 1K sessions*, or Starent Part Number [600-00-7587] *IP Services Gateway 1k Sessions*.
- Cisco PID [ASR5K-00-IG10SESS] *IP Service Gateway Base License, 10K sessions*, or Starent Part Number [600-00-7591] *IP Services Gateway 10k Sessions*.

Important: For information on additional licenses required for enhanced or customer-specific features contact your local sales representative.

For information on obtaining and installing licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

How it Works

The IPSG supports the following service modes:

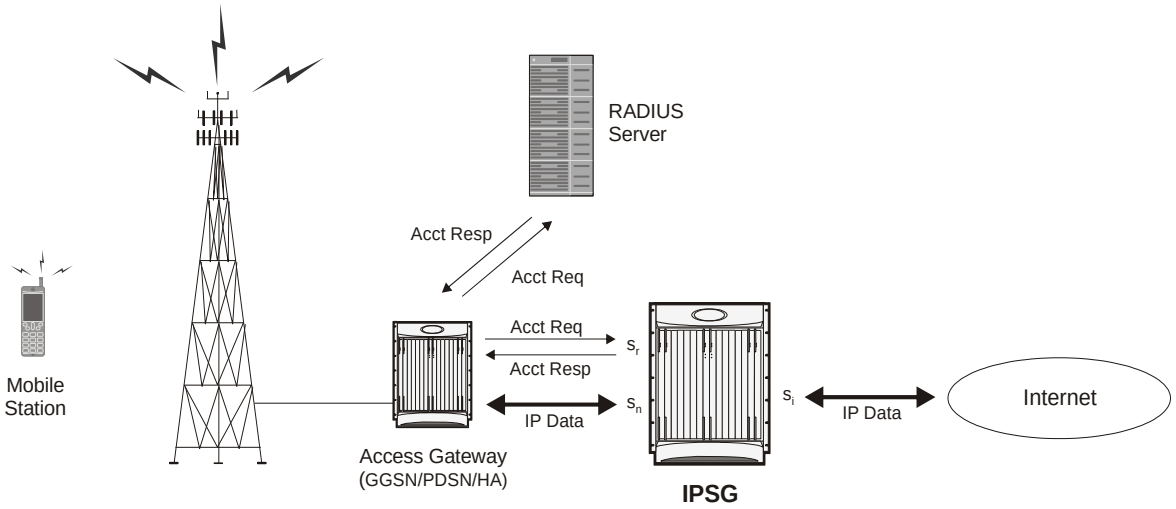
- RADIUS Server Mode
- RADIUS Snoop Mode

RADIUS Server Mode

When configured in RADIUS server mode, the IPSG inspects identical RADIUS accounting request packets sent to the RADIUS accounting server and the IPSG simultaneously.

As shown in the following figure, the IPSG inspects the RADIUS accounting request, extracts the required user information, then sends a RADIUS accounting response message back to the access gateway. The IPSG has three reference points: sn, si, and sr. The sn interface transmits/receives data packets to/from the access gateway (GGSN, HA, PDSN, etc.). The si interface transmits/receives data packets to/from the Internet or a packet data network. The sr interface receives RADIUS accounting requests from the access gateway. The system inspects the accounting request packets and extracts information to be used to determine the appropriate service(s) to apply to the flow.

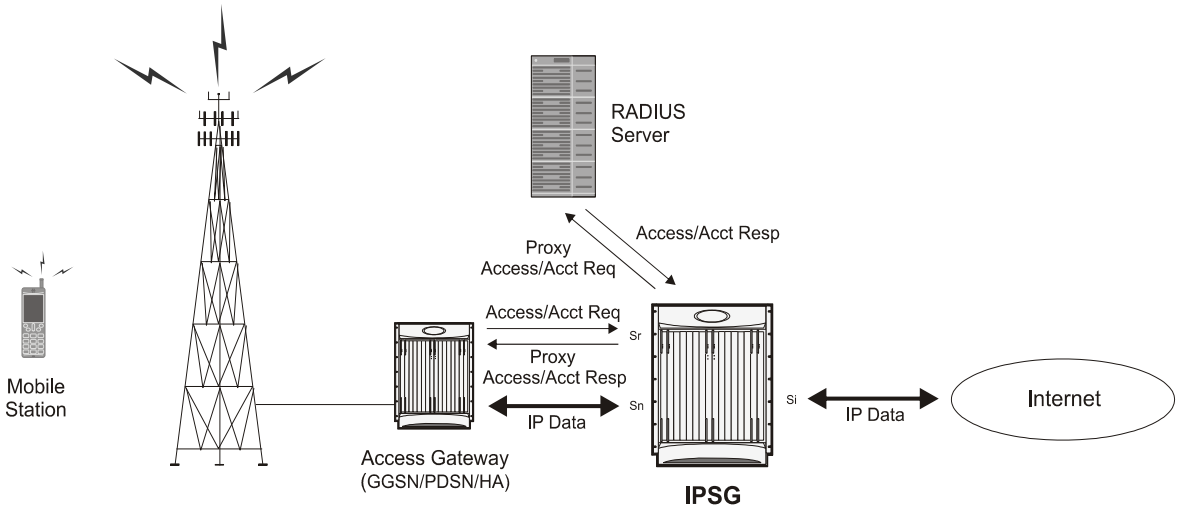
Figure 1. IPSG Message/Data Flow (RADIUS Server Mode)



RADIUS Proxy

In the event that the Access Gateway is incapable of sending two separate RADIUS Start message, the IPSG can be configured as a RADIUS Proxy. As shown in the following figure, the IPSG receives an IPSG RADIUS proxy Access request, then generates the Authentication and Accounting requests to the AAA Server.

Figure 2. IPSG Message/Data Flow (RADIUS Server Mode - RADIUS Proxy)

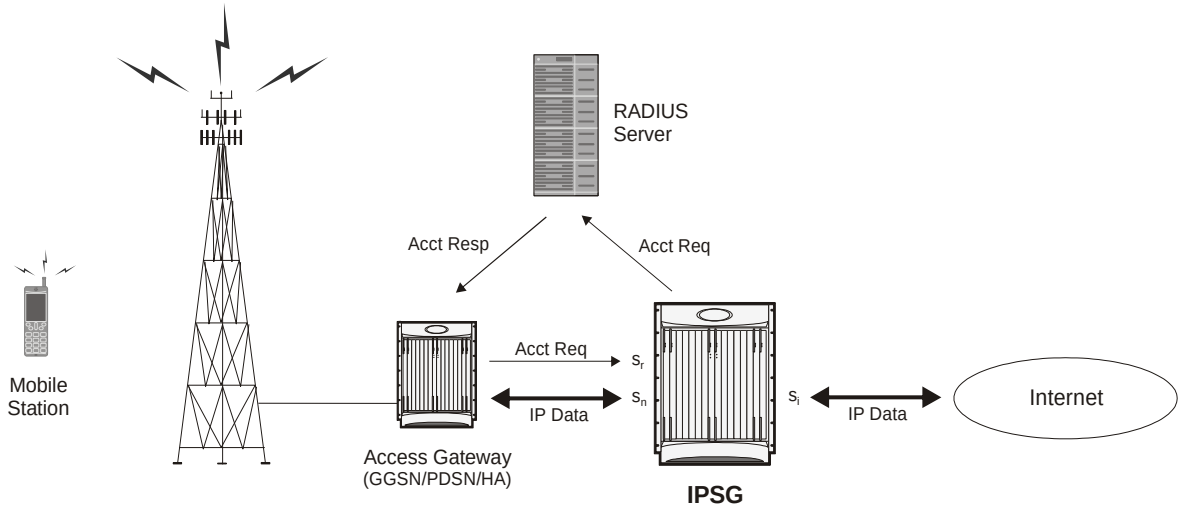


RADIUS Snoop Mode

When configured in RADIUS snoop mode, the IPSG simply inspects RADIUS accounting request packets sent to a RADIUS server through the IPSG.

As shown in the following figure, the IPSG has three reference points: sn, si, and sr. The sn interface transmits/receives data packets to/from the access gateway (GGSN, HA, PDSN, etc.). The si interface transmits/receives data packets to/from the Internet or a packet data network. The sr interface receives RADIUS accounting requests from the access gateway. The system inspects the accounting request packets and extracts information to be used to determine the appropriate service(s) to apply to the flow. Information is not extracted from the RADIUS accounting responses so they are sent directly to the access gateway by the RADIUS Server, but can also be sent back through the IPSG.

Figure 3. IPSG Message/Data Flow (RADIUS Snoop Mode)



In-line Services

As described previously, the IPSG provides a method of inspecting RADIUS packets to discover user identity for the purpose of applying enhanced services to the subsequent data flow. Internal applications such as the Enhanced Charging Service, Content Filtering, and Application Detection and Control are primary features that take advantage of the IPSG service.

Application Detection and Control

Application Detection and Control (ADC) is an in-line service feature that detects peer-to-peer protocols in real time and applies actions such as permitting, blocking, charging, bandwidth control, and TOS marking.

For more information, refer to the *Application Detection and Control Administration Guide*.

Content Filtering

Content Filtering is an in-line service feature that filters HTTP and WAP requests from mobile subscribers based on the URLs in the requests. This enables operators to filter and control the content that an individual subscriber can access, so that subscribers are inadvertently not exposed to universally unacceptable content and/or content inappropriate as per the subscribers' preferences.

For more information, refer to the *Content Filtering Services Administration Guide*.

Enhanced Charging Service

Enhanced Charging Service (ECS)/Active Charging Service (ACS) is the primary vehicle performing packet inspection and applying rules to the session which includes the delivery of enhanced services.

For more information, refer to the *Enhanced Charging Service Administration Guide*.

Enhanced Feature Support

This section describes the enhanced features supported by IPSG.

Dynamic RADIUS Extensions (Change of Authorization)

Dynamic RADIUS extension support provide operators with greater control over subscriber PDP contexts by providing the ability to dynamically redirect data traffic, and or disconnect the PDP context.

This functionality is based on the RFC 3576, Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), July 2003 standard.

The system supports the configuration and use of the following dynamic RADIUS extensions:

- Change of Authorization: The system supports CoA messages from the AAA server to change data filters associated with a subscriber session. The CoA request message from the AAA server must contain attributes to identify NAS and the subscriber session and a data filter ID for the data filter to apply to the subscriber session.
- Disconnect Message: The DM message is used to disconnect subscriber sessions in the system from a RADIUS server. The DM request message should contain necessary attributes to identify the subscriber session.

The above extensions can be used to dynamically re-direct subscriber PDP contexts to an alternate address for performing functions such as provisioning and/or account set up. This functionality is referred to as Session Redirection, or Hotlining.

Session redirection provides a means to redirect subscriber traffic to an external server by applying ACL rules to the traffic of an existing or a new subscriber session. The destination address and optionally the destination port of TCP/IP or UDP/IP packets from the subscriber are rewritten so the packet is forwarded to the designated redirected address.

Return traffic to the subscriber has the source address and port rewritten to the original values. The redirect ACL may be applied dynamically by means of the RADIUS Change of Authorization (CoA) extension.


Important: For more information on dynamic RADIUS extensions support, refer the *CoA, RADIUS, and Session Redirection (Hotlining)* appendix in the *IP Services Gateway Administration Guide*.

Gx Interface Support

To support roaming IMS subscribers in a GPRS/UMTS network, the IPSG must be able to charge only for the amount of resources consumed by the particular IMS application and bandwidth used. The IPSG must also allow for the provisioning and control of the resources used by the IMS subscriber. To facilitate this, the IPSG supports the R7 Gx interface to a Policy Control and Charging Rule Function (PCRF).

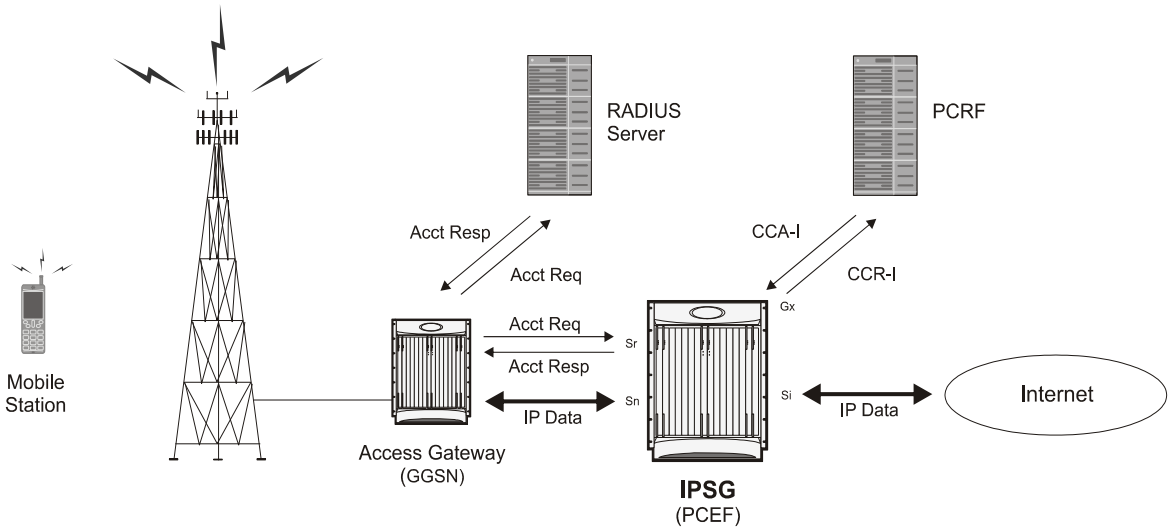
For detailed information on Gx Interface support, refer to the *Gx Interface Support* appendix in the *IP Services Gateway Administration Guide*.

Note the following for IPSG:

- Only single bearer/session concept is supported. Multiple bearer concept is not applicable.
- Only PCRF binding is applicable. PCEF binding is not applicable.

The following figure shows the interface and basic message flow of the Gx interface.

Figure 4. IPSG Message/Data Flow (RADIUS Server Mode - IMS Auth Service)



IPSG also supports IMS Authorization Service Session Recovery with the following limitations:

- Active calls only
- The number of rules recovered is limited to the following:
  - 3 flow-descriptions per charging-rule-definition
  - 3 Charging-rule-definitions per PDP context
- The above are combined limits for opened/closed gates and for uplink and downlink rules. IMSA sessions with rules more than the above are not recoverable.

Gy Interface Support

This is a Diameter protocol-based interface over which the IPSG communicates with a Charging Trigger Function (CTF) server that provides online charging data. Gy interface support provides an online charging interface that works with the ECS deep packet inspection feature. With Gy, customer traffic can be gated and billed in an “online” or “prepaid” style. Both time- and volume-based charging models are supported. In all of these models, differentiated rates can be applied to different services based on shallow or deep packet inspection.

For more information on Gy interface support, refer to the *Gy Interface Support* appendix in the *IP Services Gateway Administration Guide*.

Content Service Steering

Content Service Steering (CSS), defines how traffic is handled by the system based on the content of the data presented by a mobile subscriber. CSS can be used to direct traffic to in-line services that are internal to the system. CSS controls how subscriber data is forwarded to a particular in-line service, but does not control the content.

IPSG supports steering subscriber sessions to Content Filtering Service based on their policy setting. If a subscriber does not have a policy setting (ACL name) requiring Content Filtering, their session will bypass the Content Filtering Service and will be routed on to the destination address.

If subscriber policy entitlements indicate filtering is required for a subscriber, CSS will be used to steer subscriber sessions to the Content Filtering in-line service.

If a subscriber is using a mobile application with protocol type not supported, their session will bypass the Content Filtering Service and will be efficiently routed on to destination address.

For more information regarding CSS, refer to the *Content Service Steering* chapter in the *System Administration Guide*.

Multiple IPSG Services

Multiple IPSG services, can be configured on the system in different contexts. Both source and destination contexts should be different for the different IPSG services. Each such IPSG service functions independently as an IPSG.

Session Recovery

The Session Recovery feature provides seamless failover and reconstruction of subscriber session information in the event of a hardware or software fault within the system preventing a fully connected user session from being disconnected.

Session recovery is performed by mirroring key software processes (for example, Session Manager and AAA Manager) within the system. These mirrored processes remain in an idle state (in standby-mode), wherein they perform no processing, until they may be needed in the case of a software failure (for example, a Session Manager task aborts). The system spawns new instances of “standby mode” session and AAA Managers for each active Control Processor (CP) being used.

Additionally, other key system-level software tasks, such as VPN Manager, are performed on a physically separate packet processing card to ensure that a double software fault (for example, Session Manager and VPN Manager fails at same time on same card) cannot occur. The packet processing card used to host the VPN Manager process is in active mode and is reserved by the operating system for this sole use when session recovery is enabled.

For more information on Session Recovery, refer to the *Session Recovery* chapter in the *System Administration Guide*.

Note that the Inter-Chassis Session Recovery feature is not supported in this release.

Chapter 2
IP Services Gateway Configuration

This chapter describes how to configure the IPSG.

This chapter covers the following topics:

Configuration Requirements for the IPSG

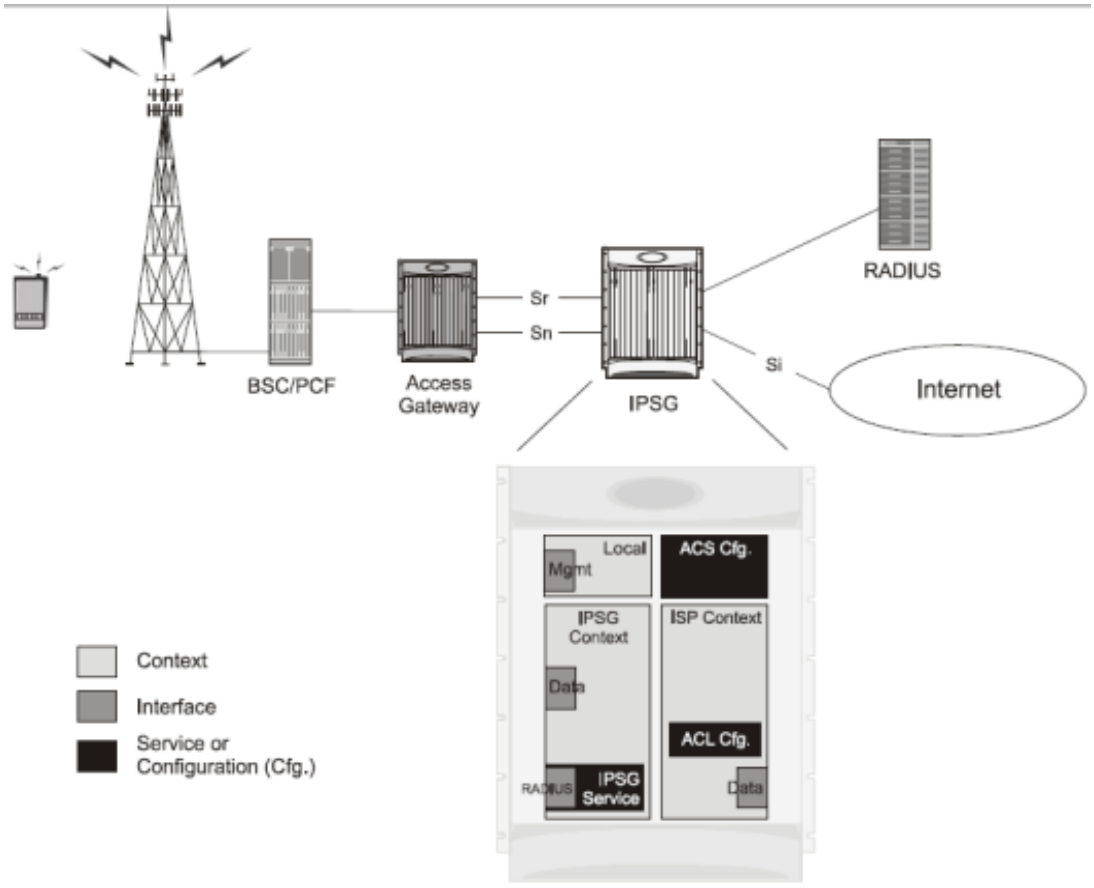
This section provides a high-level description of the configuration requirements of the IPSG.

The Snoop and Server methods use the same configuration components and differ only in how the IPSG service is configured.

The IPSG can be configured in various ways such as by creating a single context with interfaces for the RADIUS messages and both inbound and outbound data traffic. The following figure presents another method in which the IPSG context manages communication with the access gateway for both RADIUS messaging and inbound data traffic. The ISP context is responsible for all outbound data traffic.

The following figure also shows other important components such as IP access control lists (ACLs) in both contexts as well as an Enhanced Charging Service (ECS) configuration.

Figure 5. IPSG Support



Required Configuration File Components

The following configuration components are required to complete an IPSG configuration file:

- IPSG License
- Card Activations
- Local Context Modifications
    - Network Management Interface
    - Remote Management
    - Administrative Users
- Global Enhanced Charging Service Configuration
- IPSG Context
    - IPSG Service
    - RADIUS Server or Client Configuration
    - Interface for RADIUS messages to/from access gateway
    - Interface for data traffic to/from access gateway
- Service Provider Context
    - IP ACL Configuration
    - Interface for data traffic to/from access gateway
- Port Configuration (bindings)

Required Component Information

Prior to configuring the system, determine the following information:

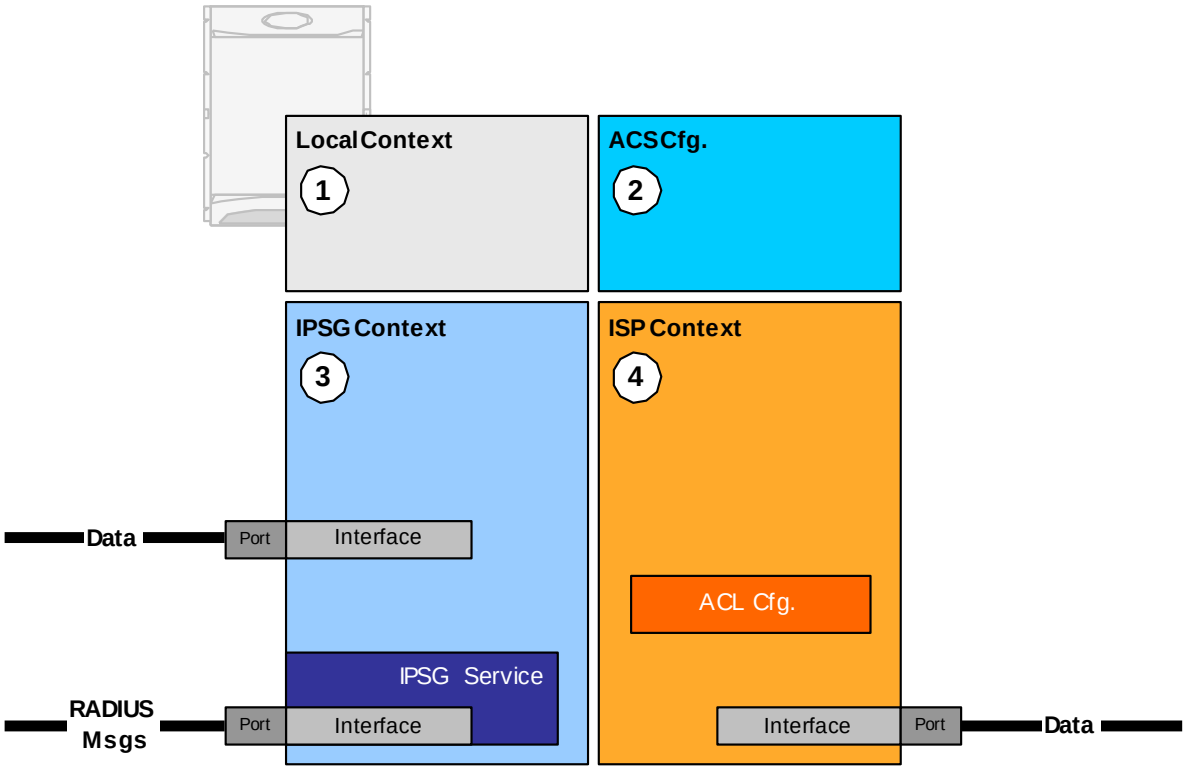
- Context names
- Service names
- Enhanced Charging Service
    - Rule definitions
    - Rulebase name
- IMS Auth Service
- RADIUS accounting client IP address, dictionary type, and shared secret (RADIUS Server Mode)
- RADIUS accounting server IP address and dictionary type (RADIUS Snoop Mode)
- All Interfaces and ports
    - Interface IP addresses
    - Interface names
    - Port names
    - Port numbers

For a complete understanding of the required information for all configuration mode commands, refer to the *Command Line Interface Reference*.

Configuring the IPSG

This section describes how to configure the IPSG to accept RADIUS accounting requests (start messages) in order to extract user information used to apply other services. The following figure illustrates the required components within the system supporting IPSG.

Figure 6. IPSG Configuration Detail



To configure the system to perform as an IPSG:

Step 1 Set initial configuration parameters such as activating processing cards and modifying the local context by referring to procedures in the *System Administration Guide*.

Step 2 Configure the global active charging parameters as described in the *Enhanced Charging Service Administration Guide*.

Step 3 Configure the system to perform as an IPSG by applying the example configurations presented in the IPSG Context and Service Configuration section.

Step 4 Configure the Service Provider context by applying the example configuration presented in the ISP Context Configuration section.

Step 5 Bind interfaces to ports as described in the *System Administration Guide*.

Step 6 Save the configuration as described in the *Verifying and Saving Your Configuration* chapter.

Important: Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

IPSG Context and Service Configuration

To configure IPSG context and service:

Step 1 Create an IPSG context and the IPSG service by applying the example configuration in one of the following sections as required:

- Option 1: RADIUS Server Mode Configuration
- Option 2: RADIUS Server with Proxy Mode Configuration
- Option 3: RADIUS Snoop Mode Configuration

Step 2 Create two interfaces within the IPSG context for communication with the access gateway by referring to the *Creating and Configuring Ethernet Interfaces and Ports* procedure in the *System Administration Guide*.

Option 1: RADIUS Server Mode Configuration

To create an IPSG context and IPSG service in RADIUS Server Mode, use the following configuration:

```
configure
   context <ipsg_context_name>
      ipsg-service <service_name> mode radius-server
         bind address <ip_address>
         radius dictionary <dictionary>
         radius accounting client <ip_address> [ encrypted ] key <secret> [
dictionary <dictionary> ] [ disconnect-message [ dest-port <port_num> ] ]
         end
```

Option 2: RADIUS Server with Proxy Mode Configuration

To create an IPSG context and IPSG service in RADIUS Server Mode with IPSG authentication and accounting proxy configuration, use the following configuration:

```
configure

   context <ipsg_context_name>

      ipsg-service <service_name> mode radius-server

         bind address <ip_address>

         radius dictionary <dictionary>

         radius accounting client <ip_address> [ encrypted ] key <secret> [
dictionary <dictionary> ] [ disconnect-message [ dest-port <port_num> ] ]

# IPSG Authentication Proxy Configuration:

         bind authentication-proxy address <ip_address>

         connection authorization [ encrypted ] password <password>

         radius dictionary <dictionary>

         radius accounting client <ip_address> [ encrypted ] key <secret> [
dictionary <dictionary> ] [ disconnect-message [ dest-port <port_num> ] ]

         exit

      aaa group default

         radius attribute nas-ip-address address <ip_address>

         radius dictionary <dictionary>

         radius server <ip_address> [ encrypted ] key <key> port <port>

         radius accounting server <ip_address> [ encrypted ] key <key> port
<port>

         exit

# IPSG Accounting Proxy Configuration:

      ipsg-service <service_name> mode radius-server

         bind accounting-proxy address <ip_address> port <port>

         radius dictionary <dictionary>

         radius accounting client <ip_address> [ encrypted ] key <secret_key> [
dictionary <dictionary> ] [ disconnect-message [ dest-port <port_num> ] ]
```

```
        exit
      aaa group default
        radius attribute nas-ip-address address <ip_address>
        radius dictionary <dictionary>
        radius accounting server <ip_address> [ encrypted ] key <key> port
<port>
        end
```

Notes:

- If both IPSG Service and client/server dictionaries are configured, the client/server dictionary takes precedence over the IPSG Service dictionary.
- If both RADIUS server and client dictionaries are configured, the client dictionary takes precedence over the server dictionary.
- For basic AAA configurations please refer to the *AAA and GTPP Interface Administration and Reference*.

Option 3: RADIUS Snoop Mode Configuration

To create an IPSG context and IPSG service in RADIUS Snoop Mode, use the following configuration:

```
configure
  context <ipsg_context_name>
    ipsg-service <service_name> mode radius-snoop
      bind
      connection authorization [ encrypted ] password <password>
      radius accounting server <ip_address>
      radius dictionary <dictionary>
      end
```

Gx Interface Configuration

For information on how to configure R7 Gx interface support, please refer to the *Configuring Rel. 7 Gx Interface* section of the *Gx Interface Support* appendix.

Note the following for IPSG:

- Only single bearer/session concept is supported. Multiple bearer concept is not applicable.
- Only PCRF binding is applicable. PCEF binding is not applicable.

Gy Interface Configuration

For information on how to configure Gy interface support, refer to the *Gy Interface Support* appendix.

ISP Context Configuration

To configure the ISP context:

Step 1 Create an ISP context as described in the Creating the ISP Context section.

Step 2 Create an interface within the ISP context to connect to the data network as described in the *System Administration Guide*.

Step 3 Create an IP access control list within the ISP context as described in the *IP Access Control Lists* chapter of the *System Administration Guide*.

Creating the ISP Context

To configure an ISP context, use the following configuration. Note that the following configuration also includes an IP route for data traffic through the IPSG context.

```
configure
   context <isp_context_name>
      subscriber default
         exit
      ip access-list <access_list>
         redirect css service <service> any
```

```
   permit any
   exit
aaa group default
   exit
ip route <ip_address/mask> <next_hop_address> <isp_data_intfc_name>
   end
```

Saving the Configuration

Refer to the *Verifying and Saving Your Configuration* chapter to save the IPSG configuration.

Chapter 3
Verifying and Saving Your Configuration

This chapter describes how to save your system configuration.

Verifying the Configuration

You can use a number of commands to verify the configuration of your feature, service, or system. Many are hierarchical in their implementation and some are specific to portions of, or specific lines in, the configuration file.

Feature Configuration

In many configurations, you have to set and verify specific features. An example includes IP address pool configuration. Using this example, enter the following commands to verify proper feature configuration:

Enter the following command to display the IP address pool configuration:

`show ip pool`

The output from this command should look similar to the sample shown below. In this example, all IP pools were configured in the *isp1* context.

```
context : isp1:

+-----Type: (P) - Public (R) - Private

 | (S) - Static (E) - Resource

 |

 |+----State: (G) - Good (D) - Pending Delete (R)-Resizing

 ||

 ||++--Priority: 0..10 (Highest (0) .. Lowest (10))

 ||||

 ||||+-Busyout: (B) - Busyout configured

 |||| |||||| vvvvv Pool Name Start Address Mask/End Address Used Avail

 ----- --------- -------------- -------------- -------- --------

PG00 ipsec 12.12.12.0 255.255.255.0 0 254 PG00

pool1 10.10.0.0 255.255.0.0 0 65534 SG00

vpnpool 192.168.1.250 192.168.1.254 0 5 Total Pool Count: 5
```

Important: To configure features on the system, use the *show* commands specifically for these features. Refer to the *Cisco Systems ASR 5000 Command Line Interface Reference* for more information.

Service Configuration

Verify that your service was created and configured properly by entering the following command:

show <*service_type*> <*service_name*>

The output is a concise listing of the service parameter settings similar to the sample displayed below. In this example, a P-GW service called *pgw* is configured.

```
Service name : pgw1

Service-Id : 1

Context : test1

Status : STARTED

Restart Counter : 8

EGTP Service : egtp1

LMA Service : Not defined

Session-Delete-Delay Timer : Enabled

Session-Delete-Delay timeout : 10000(msecs)

PLMN ID List : MCC: 100, MNC: 99

Newcall Policy : None
```

Context Configuration

Verify that your context was created and configured properly by entering the following command:

show context name <*name*>

The output shows the active context. Its ID is similar to the sample displayed below. In this example, a context named *test1* is configured.

```
Context Name     ContextID     State

------------     ---------     -----

test1            2          Active
```

System Configuration

Verify that your entire configuration file was created and configured properly by entering the following command:

show configuration

This command displays the entire configuration including the context and service configurations defined above.

Finding Configuration Errors

Identify errors in your configuration file by entering the following command:

show configuration errors

This command displays errors it finds within the configuration. For example, if you have created a service named "service1", but entered it as "srv1" in another part of the configuration, the system displays this error.

You must refine this command to specify particular sections of the configuration. Add the **section** keyword and choose a section from the help menu:

show configuration errors section ggsn-service

or

show configuration errors section aaa-config

If the configuration contains no errors, an output similar to the following is displayed:

```
##################################################################################

Displaying Global
AAA-configuration errors
##################################################################################

Total 0 error(s) in this section !
```

Saving the Configuration

Save system configuration information to a file locally or to a remote node on the network. You can use this configuration file on any other systems that require the same configuration.

Files saved locally can be stored in the CompactFlash or a PCMCIA memory card on the SMC. Files that are saved to a remote network node can be transmitted through FTP or TFTP.

Saving the Configuration on the Chassis

These instructions assume that you are at the root prompt for the Exec mode:

```
[local]host_name#
```

To save your current configuration, enter the following command:

```
save configuration url [-redundant] [-noconfirm] [showsecrets] [verbose]
```

Table 1. Command Syntax for Saving the Configuration

Keyword/Variable	Description
url	Specifies the path and name to which the configuration file is to be stored. *url* may refer to a local or a remote file. *url* must be entered using one of the following formats: • **{ /flash | /pcmcia1 | /pcmcia2 }** *[/dir] /file_name* • **file:/{ /flash | /pcmcia1 | /pcmcia2 }** *[/dir] /file_name* • **tftp://**{ *ipaddress* | *host_name* [*:port#*] } [*/directory*] */file_name* • **ftp://**[*username* [*:pwd*] *@*] { *ipaddress* | *host_name* } [*:port#*] [*/directory*] */file_name* • **sftp://**[*username* [:*pwd*] *@*] { *ipaddress* | *host_name* } [*:port#*] [*/directory*] */file_name* **/flash** corresponds to the CompactFlash on the SMC. **/pcmcia1** corresponds to PCMCIA slot 1. **/pcmcia2** corresponds to PCMCIA slot 2. *ipaddress* is the IP address of the network server. *host_name* is the network server's *hostname*. *port#* is the network server's logical port number. Defaults are: • tftp: 69 - data • ftp: 20 - data, 21 - control • sftp: 115 - data Note: *host_name* can only be used if the **networkconfig** parameter is configured for DHCP and the DHCP server returns a valid nameserv er.dx *username* is the username required to gain access to the server if necessary. *password* is the password for the specified username if required. */directory* specifies the directory where the file is located if one exists. */file_name* specifies the name of the configuration file to be saved. Note: Configuration files should be named with a .cfg extension.
-redundant	Optional: This keyword directs the system to save the CLI configuration file to the local device, defined by the url variable, and then automatically copy that same file to the like device on the Standby SMC, if available. Note: This keyword will only work for like local devices that are located on both the active and standby SMCs. For example, if you save the file to the /pcmcia1 device on the active SMC, that same type of device (a PC-Card in Slot 1 of the standby SMC) must be available. Otherwise, a failure message is displayed. Note: When saving the file to an external network (non-local) device, the system disregards this keyword.

Keyword/Variable	Description
-noconfirm	Optional: Indicates that no confirmation is to be given prior to saving the configuration information to the specified filename (if one was specified) or to the currently active configuration file (if none was specified).
showsecrets	Optional: This keyword saves the CLI configuration file with all passwords in plain text, rather than their default encrypted format.
verbose	Optional: Specifies to display every parameter that is being saved to the new configuration file.

Important: The **`-redundant`** keyword is only applicable when saving a configuration file to local devices. This command does not synchronize the local file system. If you have added, modified, or deleted other files or directories to or from a local device for the active SMC, you must synchronize the local file system on both SMCs.

To save a configuration file called *system.cfg* to a directory that was previously created called cfgfiles on the CompactFlash in the SMC, enter the following command:

```
save configuration /flash/cfgfiles/system.cfg
```

To save a configuration file called *simple_ip.cfg* to a directory called *host_name_configs*, using an FTP server with an IP address of *192.168.34.156*, on which you have an account with a username of *administrator* and a password of *secure*, use the following command:

```
save configuration
ftp://administrator:secure@192.168.34.156/host_name_configs/
simple_ip.cfg
```

To save a configuration file called *init_config.cfg* to the root directory of a TFTP server with a hostname of *config_server*, enter the following command:

```
save configuration tftp://config_server/init_config.cfg
```

Appendix A
CoA, RADIUS DM, and Session Redirection (Hotlining)

This chapter describes Change of Authorization (CoA), Disconnect Message (DM), and Session Redirect (Hotlining) support in the system.

RADIUS attributes, Access Control Lists (ACLs) and filters that are used to implement these features are discussed. The product administration guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in this Administration Guide, before using the procedures in this chapter.

Important: Not all commands and keywords/variables are available or supported. This depends on the platform type and the installed license(s).

Licensing

This feature requires the following license to be installed on the chassis:

Cisco PID [ASR5K-00-CSXXDYNR] *Dynamic Radius Extensions (CoA and PoD)*, or Starent Part Number [600-00-7518] *Dynamic Radius Extensions (CoA and PoD)*.

For information on obtaining and installing licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *Cisco ASR 5000 Series System Administration Guide*.

RADIUS Change of Authorization and Disconnect Message

This section describes how the system implements CoA and DM RADIUS messages and how to configure the system to use and respond to CoA and DM messages.

CoA Overview

The system supports CoA messages from the AAA server to change data filters associated with a subscriber session. The CoA request message from the AAA server must contain attributes to identify NAS and the subscriber session and a data filter ID for the data filter to apply to the subscriber session. The filter-id attribute (attribute ID 11) contains the name of an Access Control List (ACL). For detailed information on configuring ACLs, refer to the *IP Access Control Lists* chapter in the *Cisco ASR 5000 Series System Administration Guide*.

If the system successfully executes a CoA request, a CoA-ACK message is sent back to the RADIUS server and the data filter is applied to the subscriber session. Otherwise, a CoA-NAK message is sent with an error-cause attribute without making any changes to the subscriber session.

Important: Changing ACL and rulebase together in a single CoA is not supported. For this, two separate CoA requests can be sent through AAA server requesting for one attribute change per request.

DM Overview

The DM message is used to disconnect subscriber sessions in the system from a RADIUS server. The DM request message should contain necessary attributes to identify the subscriber session. If the system successfully disconnects the subscriber session, a DM-ACK message is sent back to the RADIUS server, otherwise, a DM-NAK message is sent with proper error reasons.

Enabling CoA and DM

To enable RADIUS Change of Authorization and Disconnect Message:

Step 1 Enable the system to listen for and respond to CoA and DM messages from the RADIUS server as described in the Enabling CoA and DM section.

Step 2 Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Step 3 View CoA and DM message statistics as described in the Viewing CoA and DM Statistics section.

Important: Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Cisco ASR 5000 Series Command Line Interface Reference* for complete information regarding all commands. Not all commands and keywords/variables are available or supported. This depends on the platform type and the installed license(s).

Enabling CoA and DM

Use the following example to enable the system to listen for and respond to CoA and DM messages from the RADIUS server:

```
configure
   context <context_name>
      radius change-authorize-nas-ip <ipv4/ipv6_address>
      end
```

Notes:

- *<context_name>* must be the name of the AAA context where you want to enable CoA and DM. The AAA context must have been configured as described in the *Configuring Context-Level AAA Functionality* section of the *Cisco ASR 5000 Series AAA and GTPP Interface Administration and Reference*.
- A number of optional keywords and variables are available for the **radius change-authorize-nas-ip** command. For more information regarding this command please refer to the *Cisco ASR 5000 Series Command Line Interface Reference*.

CoA and DM Attributes

For CoA and DM messages to be accepted and acted upon, the system and subscriber session to be affected must be identified correctly.

To identify the system, use any one of the following attributes:

- NAS-IP-Address: NAS IP address if present in the CoA/DM request should match with the NAS IP address.
- NAS-Identifier: If this attribute is present, its value should match to the nas-identifier generated for the subscriber session

To identify the subscriber session, use any one of the following attributes.

- If 3GPP2 service is configured the following attribute is used for correlation identifier:
    - 3GPP2-Correlation-ID: The values should exactly match the 3GPP2-correlation-id of the subscriber session. This is one of the preferred methods of subscriber session identification.
- If 3GPP service is configured the following attributes are used for different identifiers:
    - 3GPP-IMSI: International Mobile Subscriber Identification (IMSI) number should be validated and matched with the specified IMSI for specific PDP context.
    - 3GPP-NSAPI: Network Service Access Point Identifier (NSAPI) should match to the NSAPI specified for specific PDP context.
- User-Name: The value should exactly match the subscriber name of the session. This is one of the preferred methods of subscriber session identification.
- Framed-IP-Address: The values should exactly match the framed IP address of the session.
- Calling-station-id: The value should match the Mobile Station ID.

To specify the ACL to apply to the subscriber session, use the following attribute:

- Filter-ID: CoA only. This must be the name of an existing Access Control List. If this is present in a CoA request, the specified ACL is immediately applied to the specified subscriber session. The Context Configuration mode command, **radius attribute filter-id direction**, controls in which direction filters are applied.

The following attributes are also supported:

- Event-Timestamp: This attribute is a timestamp of when the event being logged occurred.
- If 3GPP2 service is configured following additional attributes are supported:
  - 3GPP2-Disconnect-Reason: This attribute indicates the reason for disconnecting the user. This attribute may be present in the RADIUS Disconnect-request Message from the Home Radius server to the PDSN.
  - 3GPP2-Session-Termination-Capability: When CoA and DM are enabled by issuing the radius change-authorize-nas-ip command, this attribute is included in a RADIUS Access-request message to the Home RADIUS server and contains the value 3 to indicate that the system supports both Dynamic authorization with RADIUS and Registration Revocation for Mobile IPv4. The attribute is also included in the RADIUS Access-Accept message and contains the preferred resource management mechanism by the home network, which is used for the session and may include values 1 through 3.

CoA and DM Error-Cause Attribute

The Error-Cause attribute is used to convey the results of requests to the system. This attribute is present when a CoA or DM NAK or ACK message is sent back to the RADIUS server.

The value classes of error causes are as follows:

- 0-199, 300-399 reserved
- 200-299 - successful completion
- 400-499 - errors in RADIUS server
- 500-599 - errors in NAS/Proxy

The following error cause is sent in ACK messages upon successful completion of a CoA or DM request:

- 201- Residual Session Context Removed

The following error causes are sent in NAK messages when a CoA or DM request fails:

- 401 - Unsupported Attribute
- 402 - Missing Attribute
- 403 - NAS Identification Mismatch
- 404 - Invalid Request
- 405 - Unsupported Service
- 406 - Unsupported Extension
- 501 - Administratively Prohibited
- 503 - Session Context Not Found
- 504 - Session Context Not Removable
- 506 - Resources Unavailable

Viewing CoA and DM Statistics

View CoA and DM message statistics by entering the following command:

show session subsystem facility aaamgr

The following is a sample output of this command.

```
1 AAA Managers
807 Total aaa requests                    0 Current aaa requests
379 Total aaa auth requests               0 Current aaa auth requests
  0 Total aaa auth probes                 0 Current aaa auth probes
  0 Total aaa auth keepalive              0 Current aaa auth keepalive
426 Total aaa acct requests               0 Current aaa acct requests
  0 Total aaa acct keepalive              0 Current aaa acct keepalive
379 Total aaa auth success                0 Total aaa auth failure
  0 Total aaa auth purged                 0 Total aaa auth cancelled
  0 Total auth keepalive success          0 Total auth keepalive failure
  0 Total auth keepalive purged
  0 Total aaa auth DMU challenged
367 Total radius auth requests            0 Current radius auth requests
  2 Total radius auth requests retried
  0 Total radius auth responses dropped
  0 Total local auth requests             0 Current local auth requests
 12 Total pseudo auth requests            0 Current pseudo auth requests
  0 Total null-username auth requests (rejected)
  0 Total aaa acct completed              0 Total aaa acct purged
  0 Total acct keepalive success          0 Total acct keepalive timeout
  0 Total acct keepalive purged
  0 Total aaa acct cancelled
426 Total radius acct requests            0 Current radius acct requests
  0 Total radius acct requests retried
```

```
  0 Total radius acct responses dropped

  0 Total gtpp acct requests             0 Current gtpp acct requests

  0 Total gtpp acct cancelled            0 Total gtpp acct purged

  0 Total null acct requests             0 Current null acct requests

 54 Total aaa acct sessions              5 Current aaa acct sessions

  3 Total aaa acct archived              0 Current aaa acct archived

  0 Current recovery archives            0 Current valid recovery
records

  2 Total aaa sockets opened             2 Current aaa sockets open

  0 Total aaa requests pend socket open

  0 Current aaa requests pend socket open

  0 Total radius requests pend server max-outstanding

  0 Current radius requests pend server max-outstanding

  0 Total aaa radius coa requests        0 Total aaa radius dm requests

  0 Total aaa radius coa acks            0 Total aaa radius dm acks

  0 Total aaa radius coa naks            0 Total aaa radius dm naks

  2 Total radius charg auth              0 Current radius charg auth

  0 Total radius charg auth succ         0 Total radius charg auth fail

  0 Total radius charg auth purg         0 Total radius charg auth
cancel

  0 Total radius charg acct              0 Current radius charg acct

  0 Total radius charg acct succ         0 Total radius charg acct purg

  0 Total radius charg acct cancel

357 Total gtpp charg                     0 Current gtpp charg

357 Total gtpp charg success             0 Total gtpp charg failure

  0 Total gtpp charg cancel              0 Total gtpp charg purg

  0 Total prepaid online requests        0 Current prepaid online
requests

  0 Total prepaid online success         0 Current prepaid online
failure
```

```
  0 Total prepaid online retried          0 Total prepaid online
cancelled

  0 Current prepaid online purged

  0 Total aaamgr purged requests

  0 SGSN: Total db records

  0 SGSN: Total sub db records

  0 SGSN: Total mm records

  0 SGSN: Total pdp records

  0 SGSN: Total auth records
```

Session Redirection (Hotlining)

Overview

Session redirection provides a means to redirect subscriber traffic to an external server by applying ACL rules to the traffic of an existing or a new subscriber session. The destination address and optionally the destination port of TCP/IP or UDP/IP packets from the subscriber are rewritten so the packet is forwarded to the designated redirected address. Return traffic to the subscriber has the source address and port rewritten to the original values. The redirect ACL may be applied dynamically by means of the RADIUS Change of Authorization (CoA) feature.

Note that the session redirection feature is only intended to redirect a very small subset of subscribers at any given time. The data structures allocated for this feature are kept to the minimum to avoid large memory overhead in the session managers.

Operation

ACL Rule

An ACL rule named **readdress server** supports redirection of subscriber sessions. The ACL containing this rule must be configured in the destination context of the user. Only TCP and UDP protocol packets are supported. The ACL rule allows specifying the redirected address and an optional port. The source and destination address and ports (with respect to the traffic originating from the subscriber) may be wildcarded. If the redirected port is not specified, the traffic will be redirected to the same port as the original destination port in the datagrams. For detailed information on configuring ACLs, refer to the *IP Access Control Lists* chapter in the *Cisco ASR 5000 Series System Administration Guide*. For more information on **readdress server**, refer to the *ACL Configuration Mode Commands* chapter of the *Cisco ASR 5000 Series Command Line Interface Reference*.

Redirecting Subscriber Sessions

An ACL with the **readdress server** rule is applied to an existing subscriber session through CoA messages from the RADIUS server. The CoA message contains the 3GPP2-Correlation-ID, User-Name, Acct-Session-ID, or Framed-IP-Address attributes to identify the subscriber session. The CoA message also contains the Filter-Id attribute which specifies the name of the ACL with the r**eaddress server** rule. This enables applying the ACL dynamically to existing subscriber sessions. By default, the ACL is applied as both the input and output filter for the matching subscriber unless the Filter-Id in the CoA message bears the prefix **in:** or **out:**.

For information on CoA messages and how they are implemented in the system, refer to the RADIUS Change of Authorization and Disconnect Message section.

Important: Changing ACL and rulebase together in a single CoA is not supported. For this, two separate CoA requests can be sent through AAA server requesting for one attribute change per request.

Session Limits On Redirection

To limit the amount of memory consumed by a session manager a limit of 2000 redirected session entries per session manager is allocated. This limit is equally shared by the set of subscribers who are currently being redirected. Whenever a redirected session entry is subject to revocation from a subscriber due to an insufficient number of available session entries, the least recently used entry is revoked.

Stopping Redirection

The redirected session entries for a subscriber remain active until a CoA message issued from the RADIUS server specifies a filter that does not contain the readdress server ACL rule. When this happens, the redirected session entries for the subscriber are deleted.

All redirected session entries are also deleted when the subscriber disconnects.

Handling IP Fragments

Since TCP/UDP port numbers are part of the redirection mechanism, fragmented IP datagrams must be reassembled before being redirected. Reassembly is particularly necessary when fragments are sent out of order. The session manager performs reassembly of datagrams and reassembly is attempted only when a datagram matches the redirect server ACL rule. To limit memory usage, only up to 10 different datagrams may be concurrently reassembled for a subscriber. Any additional requests cause the oldest datagram being reassembled to be discarded. The reassembly timeout is set to 2 seconds. In addition, the limit on the total number of fragments being reassembled by a session manager is set to 1000. If this limit is reached, the oldest datagram being reassembled in the session manager and its fragment list are discarded. These limits are not configurable.

Recovery

When a session manager dies, the ACL rules are recovered. The session redirect entries have to be re-created when the MN initiates new traffic for the session. Therefore when a crash occurs, traffic from the Internet side is not redirected to the MN.

AAA Accounting

Where destination-based accounting is implemented, traffic from the subscriber is accounted for using the original destination address and not the redirected address.

Viewing the Redirected Session Entries for a Subscriber

View the redirected session entries for a subscriber by entering the following command:

show subscribers debug-info { callid <*id*> **| msid** <*id*> **| username** <*name*> **}**

The following command displays debug information for a subscriber with the MSID 0000012345:

show subscribers debug-info msid 0000012345

The following is a sample output of this command:

```
username: user1 callid: 01ca11b1 msid: 0000100003
 Card/Cpu: 4/2
 Sessmgr Instance: 7
 Primary callline:
 Redundancy Status: Original Session
 Checkpoints Attempts Success Last-Attempt Last-Success
 Full: 27 26 15700ms 15700ms
 Micro: 76 76 4200ms 4200ms
 Current state: SMGR_STATE_CONNECTED
 FSM Event trace:
 State Event
 SMGR_STATE_OPEN SMGR_EVT_NEWCALL SMGR_STATE_NEWCALL_ARRIVED
SMGR_EVT_ANSWER_CALL SMGR_STATE_NEWCALL_ANSWERED SMGR_EVT_LINE_CONNECTED
SMGR_STATE_LINE_CONNECTED SMGR_EVT_LINK_CONTROL_UP SMGR_STATE_LINE_CONNECTED
SMGR_EVT_AUTH_REQ
 SMGR_STATE_LINE_CONNECTED SMGR_EVT_IPADDR_ALLOC_SUCCESS
 SMGR_STATE_LINE_CONNECTED SMGR_EVT_AUTH_SUCCESS
 SMGR_STATE_LINE_CONNECTED SMGR_EVT_UPDATE_SESS_CONFIG
 SMGR_STATE_LINE_CONNECTED SMGR_EVT_LOWER_LAYER_UP
Data Reorder statistics
 Total timer expiry: 0 Total flush (tmr expiry): 0
 Total no buffers: 0 Total flush (no buffers): 0
 Total flush (queue full): 0 Total flush (out of range):0
 Total flush (svc change): 0 Total out-of-seq pkt drop: 0
```

```
          Total out-of-seq arrived: 0
 IPv4 Reassembly Statistics:
  Success: 0 In Progress: 0
  Failure (timeout): 0 Failure (no buffers): 0
  Failure (other reasons): 0
 Redirected Session Entries:
  Allowed: 2000 Current: 0
  Added: 0 Deleted: 0
  Revoked for use by different subscriber: 0
  Peer callline:
  Redundancy Status: Original Session
  Checkpoints Attempts Success Last-Attempt Last-Success
  Full: 0 0 0ms 0ms
  Micro: 0 0 0ms 0ms
  Current state: SMGR_STATE_CONNECTED
  FSM Event trace:
  State Event
  SMGR_STATE_OPEN SMGR_EVT_MAKECALL
  SMGR_STATE_MAKECALL_PENDING SMGR_EVT_LINE_CONNECTED
  SMGR_STATE_LINE_CONNECTED SMGR_EVT_LOWER_LAYER_UP
  SMGR_STATE_CONNECTED SMGR_EVT_AUTH_REQ
  SMGR_STATE_CONNECTED SMGR_EVT_AUTH_SUCCESS
  SMGR_STATE_CONNECTED SMGR_EVT_REQ_SUB_SESSION
  SMGR_STATE_CONNECTED SMGR_EVT_RSP_SUB_SESSION
 username: user1 callid: 01ca11b1 msid: 0000100003
  Card/Cpu: 4/2
  Sessmgr Instance: 7
  Primary callline:
  Redundancy Status: Original Session
```

```
 Checkpoints Attempts Success Last-Attempt Last-Success
 Full: 27 26 15700ms 15700ms
 Micro: 76 76 4200ms 4200ms
 Current state: SMGR_STATE_CONNECTED
 FSM Event trace:
 State Event
 SMGR_STATE_OPEN SMGR_EVT_NEWCALL
 SMGR_STATE_NEWCALL_ARRIVED SMGR_EVT_ANSWER_CALL
 SMGR_STATE_NEWCALL_ANSWERED SMGR_EVT_LINE_CONNECTED
 SMGR_STATE_LINE_CONNECTED SMGR_EVT_LINK_CONTROL_UP
 SMGR_STATE_LINE_CONNECTED SMGR_EVT_AUTH_REQ
 SMGR_STATE_LINE_CONNECTED SMGR_EVT_IPADDR_ALLOC_SUCCESS
 SMGR_STATE_LINE_CONNECTED SMGR_EVT_AUTH_SUCCESS
 SMGR_STATE_LINE_CONNECTED SMGR_EVT_UPDATE_SESS_CONFIG
 SMGR_STATE_LINE_CONNECTED SMGR_EVT_LOWER_LAYER_UP
Data Reorder statistics
 Total timer expiry: 0 Total flush (tmr expiry): 0
 Total no buffers: 0 Total flush (no buffers): 0
 Total flush (queue full): 0 Total flush (out of range):0
 Total flush (svc change): 0 Total out-of-seq pkt drop: 0
         Total out-of-seq arrived: 0
IPv4 Reassembly Statistics:
 Success: 0 In Progress: 0
 Failure (timeout): 0 Failure (no buffers): 0
 Failure (other reasons): 0
Redirected Session Entries:
 Allowed: 2000 Current: 0
 Added: 0 Deleted: 0
 Revoked for use by different subscriber: 0
```

```
Peer callline:
 Redundancy Status: Original Session
 Checkpoints Attempts Success Last-Attempt Last-Success
 Full: 0 0 0ms 0ms
 Micro: 0 0 0ms 0ms
 Current state: SMGR_STATE_CONNECTED
 FSM Event trace:
 State Event
 SMGR_STATE_OPEN SMGR_EVT_MAKECALL
 SMGR_STATE_MAKECALL_PENDING SMGR_EVT_LINE_CONNECTED
 SMGR_STATE_LINE_CONNECTED SMGR_EVT_LOWER_LAYER_UP
 SMGR_STATE_CONNECTED SMGR_EVT_AUTH_REQ
 SMGR_STATE_CONNECTED SMGR_EVT_AUTH_SUCCESS
 SMGR_STATE_CONNECTED SMGR_EVT_REQ_SUB_SESSION
 SMGR_STATE_CONNECTED SMGR_EVT_RSP_SUB_SESSION
 SMGR_STATE_CONNECTED SMGR_EVT_ADD_SUB_SESSION
 SMGR_STATE_CONNECTED SMGR_EVT_AUTH_REQ
 SMGR_STATE_CONNECTED SMGR_EVT_AUTH_SUCCESS
 Data Reorder statistics
 Total timer expiry: 0 Total flush (tmr expiry): 0
 Total no buffers: 0 Total flush (no buffers): 0
 Total flush (queue full): 0 Total flush (out of range):0
 Total flush (svc change): 0 Total out-of-seq pkt drop: 0
 Total out-of-seq arrived: 0
 IPv4 Reassembly Statistics:
 Success: 0 In Progress: 0
 Failure (timeout): 0 Failure (no buffers): 0
 Failure (other reasons): 0
 Redirected Session Entries:
```

```
Allowed: 2000 Current: 0
Added: 0 Deleted: 0
Revoked for use by different subscriber: 0
```

Appendix B
Gx Interface Support

This chapter provides information on configuring Gx interface to support policy and charging control for subscribers.

The IMS service provides application support for transport of voice, video, and data independent of access support. Roaming IMS subscribers require apart from other functionality sufficient, uninterrupted, consistent, and seamless user experience during an application session. It is also important that a subscriber gets charged only for the resources consumed by the particular IMS application used.

It is recommended that before using the procedures in this chapter you select the configuration example that best meets your service model, and configure the required elements for that model as described in this Administration Guide.

The following topics are covered in this chapter:

Rel. 6 Gx Interface

Rel. 6 Gx interface support is available on the Cisco ASR 5000 platform running StarOS 8.0 and later releases for the following products:

- GGSN
- IPSG

This section describes the following topics:

Introduction

In GPRS/UMTS networks, the client functionality lies with the GGSN/IPSG, therefore in the IMS authorization scenario it is also called Access Gateway (AGW).

The provisioning of charging rules that are based on the dynamic analysis of flows used for the IMS session is carried out over the Gx interface. In 3GPP, Rel. 6 the Gx is an interface between Access Gateway functioning as Traffic Plane Function (TPF) and the Charging Rule Function (CRF). It is based on the Diameter Base Protocol (DIABASE) and the Diameter Credit Control Application (DCCA) standard. The GGSN/TPF acts as the client where as the CRF contains the Diameter server functionality.

The AGW is required to perform query, in reply to which the servers provision certain policy or rules that are enforced at the AGW for that particular subscriber session. The CRF analyzes the IP flow data, which in turn has been retrieved from the Session Description Protocol (SDP) data exchanged during IMS session establishment.

Important: In addition to standard Gx interface functionality, the Gx interface implemented here provides support of SBLP with additional AVPs in custom DPCA dictionaries. For more information on customer-specific support contact your local technical support representative. In view of required flow bandwidth and QoS, the system provides enhanced support for use of Service Based Local Policy (SBLP) to provision and control the resources used by the IMS subscriber. SBLP is based on the dynamic parameters such as the media/traffic flows for data transport, network conditions and static parameters, such as subscriber configuration and category. It also provides Flow-based Charging (FBC) mechanism to charge the subscriber dynamically based on content usage. With this additional functionality, the Cisco Systems Gateway can act as an Enhanced Policy Decision Function (E-PDF).

Licensing

This feature requires the following license to be installed on the chassis:

Cisco PID [ASR5K-00-CS01PIF] *Policy Interface, 1K sessions*, or Starent Part Number [600-00-7585] *Dynamic Policy Interface* — license for IMS Authorization Service feature.

For information on obtaining and installing licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *Cisco ASR 5000 Series System Administration Guide*.

Supported Standards

The Rel 6. Gx interface support is based on the following standards and request for comments (RFCs):

- 3GPP TS 29.210, Charging rule provisioning over Gx interface
- RFC 3588, Diameter Base Protocol; September 2003
- RFC 4006, Diameter Credit-Control Application; August 2005

In addition to the above RFCs and standards, IMS Authorization partially supports 3GPP TS 29.212 for Policy and Charging Control over Gx reference point functionality.

Supported Networks and Platforms

This feature is supported on all ASR 5000 Series Platforms with StarOS Release 8.0 or later running GGSN service for the core network services.

How it Works

This section describes the IMS authorization and dynamic policy support in GPRS/UMTS networks.

The following figure and table explain the IMS authorization process between a system and IMS components that is initiated by the MN.

In the case of GGSN, the DPCA is the Gx interface to the Control and Charging Rule Function (CRF). In this context CRF will act as Enhanced Policy Decision Function (E-PDF). The CRF may reside in Proxy-Call Session Control Function (P-CSCF) or on stand-alone system.

The interface between IMSA with CRF is the Gx interface, and between Session Manager and Online Charging Service (OCS) is the Gy interface.

Note that the IMS Authorization (IMSA) service and Diameter Policy Control Application (DPCA) are part of Session Manager on the system, and separated in the following figure for illustration purpose only.

Figure 7. Rel. 6 Gx IMS Authorization Call Flow

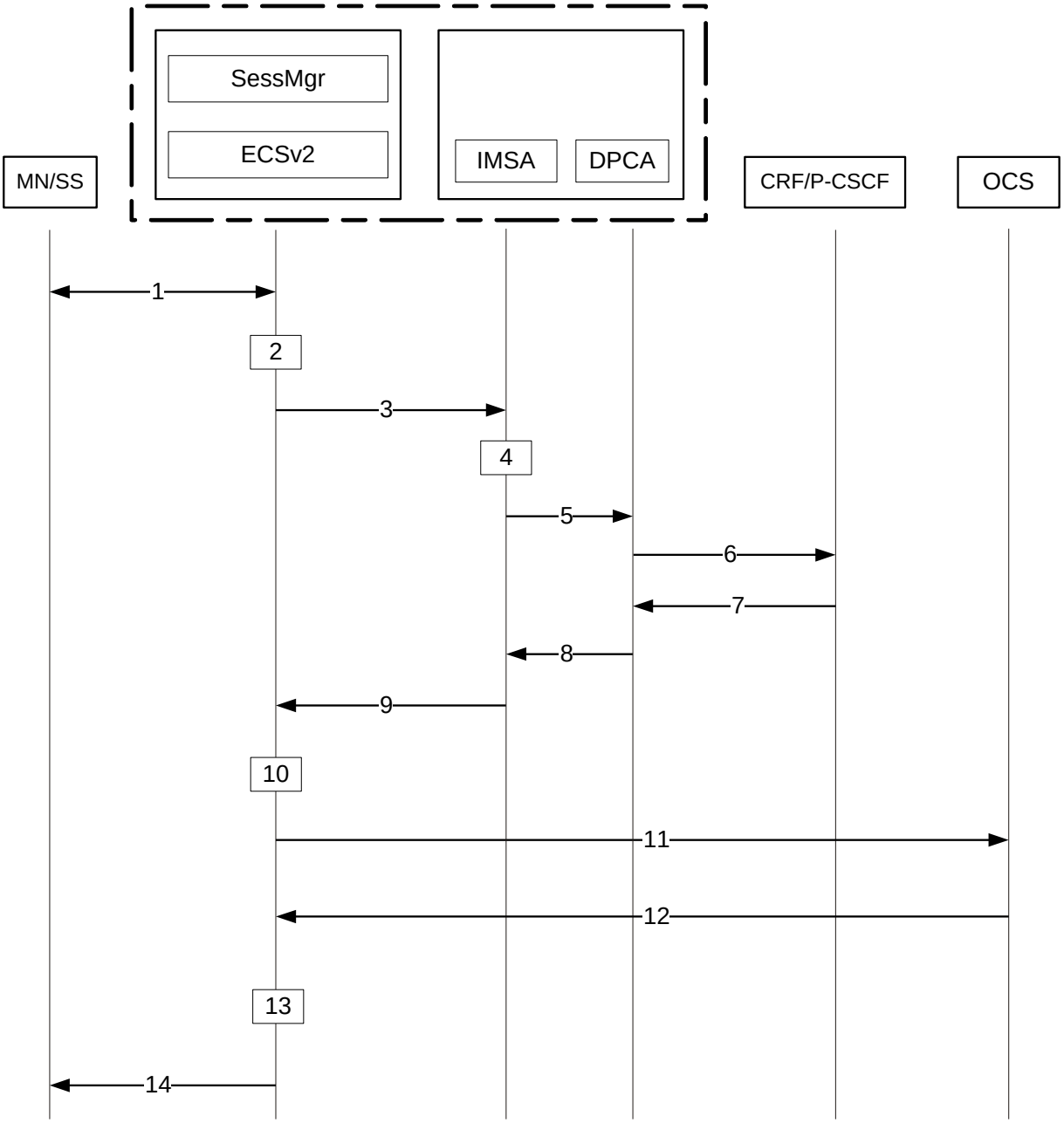


Table 2. Rel. 6 Gx IMS Authorization Call flow Description

Step	Description
1	IMS subscriber (MN) sends request for primary PDP context activation/creation.
2	Session manager allocates IP address to MN.

Step	Description
3	Session manager sends IMS authorization request to IMS Authorization service (IMSA).
4	IMSA creates a session with the CRF on the basis of CRF configuration.
5	IMSA sends request to DPCA module to issue the authorization request to selected CRF.
6	DPCA sends a CCR-initial message to the selected CRF. This message includes the IP address allocated to MN.
7	CCA message sent to DPCA. If a preconfigured rule set for the PDP context is provided in CRF, it sends that charging rules to DPCA in CCA message.
8	DPCA module calls the callback function registered with it by IMSA.
9	After processing the charging rules, IMSA sends Policy Authorization Complete message to session manager.
10	The rules received in CCA message are used for dynamic rule configuration structure and session manager sends the message to ECS.
11	ECS installs the rules and performs credit authorization by sending CCR-Initial to Online Charging System (OCS) with CC-Request-Type set to INITIAL_REQUEST to open the credit control session. This request includes the active rule base ID and 3GPP specific attributes (for example, APN, QoS and so on).
12	OCS returns a CCA-Initial message to activate the statically configured rulebase and includes preemptive credit quotas.
13	ECS responds to session manager with the response message for dynamic rule configuration.
14	On the basis of response for the PDP context authorization, Session Manager sends the response to the MN and activates/rejects the call.

Configuring Rel. 6 Gx Interface

To configure Rel. 6 Gx interface functionality:

Step 1 Configure the IMS Authorization Service at the context level for an IMS subscriber in GPRS/UMTS network as described in the Configuring IMS Authorization Service at Context Level section.

Step 2 Verify your configuration, as described in the Verifying IMS Authorization Service Configuration section.

Step 3 Configure an APN within the same context to use the IMS Authorization service for an IMS subscriber as described in the Applying IMS Authorization Service to an APN section.

Step 4 Verify your configuration as described in the Verifying Subscriber Configuration section.

Step 5 Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Important: Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Cisco ASR 5000 Series Command Line Interface Reference* for complete information regarding all commands.

Configuring IMS Authorization Service at Context Level

Use the following example to configure IMS Authorization Service at context level for IMS subscribers in GPRS/UMTS networks:

```
configure

   context <context_name>

      ims-auth-service <imsa_service_name>

         p-cscf table { 1 | 2 } row-precedence <precedence_value> { address
<ip_address> | ipv6-address <ipv6_address> }

         p-cscf discovery { table { 1 | 2 } [ algorithm { ip-address-modulus |
msisdn-modulus | round-robin } ] | diameter-configured }

         policy-control

            diameter origin endpoint <endpoint_name>

            diameter dictionary <dictionary>

            failure-handling cc-request-type { any-request | initial-request |
terminate-request | update-request } { diameter-result-code { any-error |
<result_code> [ to <end_result_code> ] } } { continue | retry-and-terminate |
terminate }

            diameter host-select row-precedence <precedence_value> table { 1 | 2
} host <host_name> [ realm <realm_name> ] [ secondary host <host_name> [ realm
<realm_name> ] ]

            diameter host-select reselect subscriber-limit <subscriber_limit>
time-interval <duration>

            diameter host-select table { 1 | 2 } algorithm { ip-address-modulus
| msisdn-modulus | round-robin }

            end
```

Notes:

- *<context_name>* must be the name of the context where you want to enable IMS Authorization Service.
- *<imsa_service_name>* must be the name of the IMS Authorization Service to be configured for the Gx interface authentication.
- A maximum of 16 authorization services can be configured globally in a system. There is also a system limit for maximum number of total configured services.
- Secondary P-CSCF IP address can be configured in the P-CSCF table. Refer to the *Cisco ASR 5000 Series Command Line Interface Reference* for more information on the **p-cscf table** command.
- To enable Rel. 6 Gx interface support, specific Diameter dictionary must be configured. For information on the Diameter dictionary to use, please contact your local service representative.
- *Optional:* To configure the quality of service (QoS) update timeout for a subscriber, in the IMS Authorization Service Configuration Mode, enter the following command:

qos-update-timeout *<timeout_duration>*

- *Optional:* To configure signalling restrictions, in the IMS Authorization Service Configuration Mode, enter the following commands:

  signaling-flag { deny | permit }

  signaling-flow permit server-address *<ip_address>* **[server-port {** *<port_number>* **| range** *<start_number>* **to** *<end_number>* **}] [description** *<string>* **]**

- *Optional:* To configure action on packets that do not match any policy gates in the general purpose PDP context, in the IMS Authorization Service Configuration Mode, enter the following command:

  traffic-policy general-pdp-context no-matching-gates direction { downlink | uplink } { forward | discard }

- *Optional:* To configure the algorithm to select Diameter host table, in the Policy Control Configuration Mode, enter the following command:

  diameter host-select table { 1 | 2 } algorithm { ip-address-modulus | msisdn-modulus | round-robin }

Verifying IMS Authorization Service Configuration

To verify the IMS Authorization Service configuration:

Step 1 Change to the context where you enabled IMS Authorization Service by entering the following command:

context *<context_name>*

Step 2 Verify the IMS Authorization Service's configurations by entering the following command:

show ims-authorization service name *<imsa_service_name>*

Applying IMS Authorization Service to an APN

After configuring IMS Authorization service at the context-level, an APN within the same context must be configured to use the IMS Authorization service for an IMS subscriber.

Use the following example to apply IMS Authorization service functionality to a previously configured APN within the context configured in the Configuring IMS Authorization Service section.

```
configure
   context <context_name>
      apn <apn_name>
         ims-auth-service <imsa_service_name>
         end
```

Notes:

- *<context_name>* must be the name of the context in which the IMS Authorization service was configured.
- *<imsa_service_name>* must be the name of the IMS Authorization Service configured for IMS authentication in the context.

Verifying Subscriber Configuration

Verify the IMS Authorization Service configuration for subscriber(s) by entering the following command:

show subscribers ims-auth-service *<imsa_service_name>*

<imsa_service_name> must be the name of the IMS Authorization Service configured for IMS authentication.

Rel. 7 Gx Interface

Rel. 7 Gx interface support is available on the Cisco ASR 5000 platform running StarOS 8.1 or StarOS 9.0 and later releases for the following products:

- GGSN
- IPSG

This section describes the following topics:

Introduction

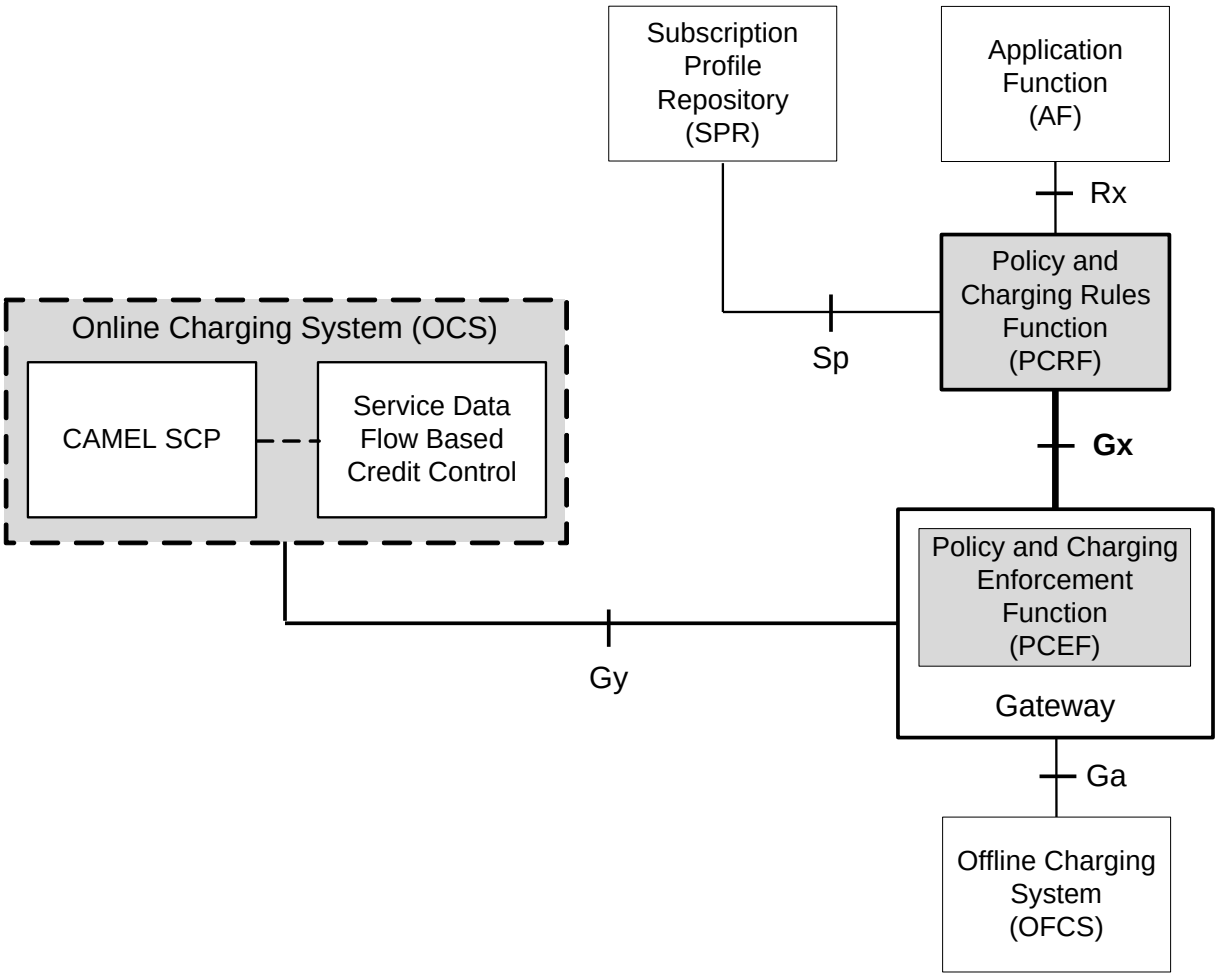
For IMS deployment in GPRS/UMTS networks the system uses Rel. 7 Gx interface for policy-based admission control support and flow-based charging. The Rel. 7 Gx interface supports enforcing policy control features like gating, bandwidth limiting, and so on, and also supports flow-based charging. This is accomplished via dynamically provisioned Policy Control and Charging (PCC) rules. These PCC rules are used to identify Service Data Flows (SDF) and do charging. Other parameters associated with the rules are used to enforce policy control.

The PCC architecture allows operators to perform service-based QoS policy, and flow-based charging control. In the PCC architecture, this is accomplished mainly by the Policy and Charging Enforcement Function (PCEF)/Cisco Systems GGSN and the Policy and Charging Rules Function (PCRF).

In GPRS/UMTS networks, the client functionality lies with the GGSN, therefore in the IMS authorization scenario it is also called the Gateway. In the following figure, Gateway is the Cisco Systems GGSN, and the PCEF function is provided by Enhanced Charging Service (ECS). The Rel 7. Gx interface is implemented as a Diameter connection. The Gx messages mostly involve installing/modifying/removing dynamic rules and activating/deactivating predefined rules.

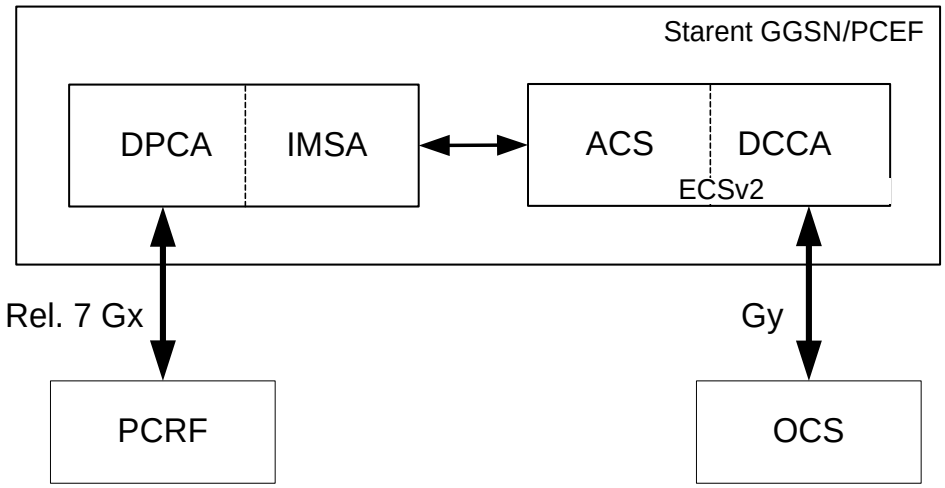
The Rel. 7 Gx reference point is located between the Gateway and the PCRF. This reference point is used for provisioning and removal of PCC rules from the PCRF to the Gateway, and the transmission of traffic plane events from the Gateway to the PCRF. The Gx reference point can be used for charging control, policy control, or both by applying AVPs relevant to the application. The following figure shows the reference points between various elements involved in the policy and charging architecture.

Figure 8. PCC Logical Architecture



Within the Gateway, the IMSA and DPCA modules handle the Gx protocol related functions (at the SessMgr) and the policy enforcement and charging happens at ECS. The Gy protocol related functions are handled within the DCCA module (at the ECS). The following figure shows the interaction between components within the Gateway.

Figure 9. PCC Architecture within Cisco PCEF



Supported Networks and Platforms

This feature is supported on all ASR 5000 Series Platforms with StarOS Release 8.1 and later running GGSN service for the core network services.

Licensing

This feature requires the following licenses to be installed on the chassis:

- Cisco PID [ASR5K-00-CS01PIF] *Policy Interface, 1K sessions*, or Starent Part Number [600-00-7585] *Dynamic Policy Interface* — license for IMS Authorization Service feature.
- Cisco PID [ASR5K-00-CS01ECG2] *Enhanced Charging Bundle 2 1k Sessions*, or Starent Part Number [600-00-7574] *Enhanced Charging Bundle 2 1k Sessions* — To enable and configure Diameter and ECS functionality.

For information on obtaining and installing licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *Cisco ASR 5000 Series System Administration Guide*.

Supported Standards

The Rel 7. Gx interface support is based on the following standards and RFCs:

- 3GPP TS 23.203 V7.6.0 (2008-03): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 7)
- 3GPP TS 29.212 V7.8.0 (2009-03): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 7)
- 3GPP TS 29.213 V7.4.0 (2008-03): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control signalling flows and QoS parameter mapping; (Release 7)
- RFC 3588, Diameter Base Protocol; September 2003
- RFC 4006, Diameter Credit-Control Application; August 2005

Terminology and Definitions

This section describes features and terminology pertaining to Rel. 7 Gx functionality.

Policy Control

The process whereby the PCRF indicates to the PCEF how to control the IP-CAN bearer.

Policy control comprises the following functions:

- **Binding:** Binding is the generation of an association between a Service Data Flow (SDF) and the IP CAN bearer (for GPRS a PDP context) transporting that SDF.

  The QoS demand in the PCC rule, as well as the SDF template are input for the bearer binding. The selected bearer will have the same QoS Class as the one indicated by the PCC rule.

  Depending on the type of IP-CAN and bearer control mode, bearer binding can be executed either by the PCRF, or both PCRF and PCEF.

  - For UE-only IP-CAN bearer establishment mode, the PCRF performs bearer binding. When the PCRF performs bearer binding, it indicates the bearer (PDP context) by means of Bearer ID. The Bearer ID uniquely identifies the bearer within the PDP session.
  - For UE/NW IP-CAN bearer establishment mode, the PCRF performs the binding of the PCC rules for user controlled services, while the PCEF performs the binding of the PCC rules for the network-controlled services.
- **Gating Control:** Gating control is the blocking or allowing of packets, belonging to an SDF, to pass through to the desired endpoint. A gate is described within a PCC rule and gating control is applied on a per SDF basis. The commands to open or close the gate leads to the enabling or disabling of the passage for corresponding IP

packets. If the gate is closed, all packets of the related IP flows are dropped. If the gate is opened, the packets of the related IP flows are allowed to be forwarded.

- **Event Reporting**: Event reporting is the notification of and reaction to application events to trigger new behavior in the user plane as well as the reporting of events related to the resources in the Gateway (PCEF).
  - Event triggers may be used to determine which IP-CAN session modification or specific event causes the PCEF to re-request PCC rules. Although event trigger reporting from PCEF to PCRF can apply for an IP CAN session or bearer depending on the particular event, provisioning of event triggers will be done at session level.

    Note that in 11.0 and later releases, RAR with unknown event triggers are silently ignored and responded with DIAMETER_SUCCESS. In earlier releases, when unknown event triggers were received in the RAR command from PCRF, invalid AVP result code was set in the RAA command.
  - The Event Reporting Function (ERF) receives event triggers from PCRF during the Provision of PCC Rules procedure and performs event trigger detection. When an event matching the received event trigger occurs, the ERF reports the occurred event to the PCRF. If the provided event triggers are associated with certain parameter values then the ERF includes those values in the response back to the PCRF. The Event Reporting Function is located in the PCEF.

    Important: In this release, event triggers "IP-CAN_CHANGE" and "MAX_NR_BEARERS_REACHED" are not supported.

- **QoS Control:** QoS control is the authorization and enforcement of the maximum QoS that is authorized for a SDF or an IP-CAN bearer or a QoS Class Identifier (QCI). In case of an aggregation of multiple SDFs (for GPRS a PDP context), the combination of the authorized QoS information of the individual SDFs is provided as the authorized QoS for this aggregate.
  - QoS control per SDF allows the PCC architecture to provide the PCEF with the authorized QoS to be enforced for each specific SDF.
  - The enforcement of the authorized QoS of the IP-CAN bearer may lead to a downgrading or upgrading of the requested bearer QoS by the Gateway (PCEF) as part of a UE-initiated IP-CAN bearer establishment or modification. Alternatively, the enforcement of the authorized QoS may, depending on operator policy and network capabilities, lead to network-initiated IP-CAN bearer establishment or modification. If the PCRF provides authorized QoS for both, the IP-CAN bearer and PCC rule(s), the enforcement of authorized QoS of the individual PCC rules takes place first.
  - QoS authorization information may be dynamically provisioned by the PCRF, or it can be a predefined PCC rule in the PCEF. In case the PCRF provides PCC rules dynamically, authorized QoS information for the IP-CAN bearer (combined QoS) may be provided. For a predefined PCC rule within the PCEF, the authorized QoS information takes affect when the PCC rule is activated. The PCEF combines the different sets of authorized QoS information, that is the information received from the PCRF and the information corresponding to the predefined PCC rules. The PCRF knows the authorized QoS information of the predefined PCC rules and takes this information into account when activating them. This ensures that the combined authorized QoS of a set of PCC rules that are activated by the PCRF is within the limitations given by the subscription and operator policies regardless of whether these PCC rules are dynamically provided, predefined, or both.

    Important: In this release, QoS Resource Reservation is not supported.

Supported Features:

- Provisioning and Policy Enforcement of Authorized QoS: The PCRF may provide authorized QoS to the PCEF. The authorized QoS provides appropriate values for resources to be enforced.
- Provisioning of "Authorized QoS" Per IP CAN Bearer: The authorized QoS per IP-CAN bearer is used if the bearer binding is performed by the PCRF.
- Policy Enforcement for "Authorized QoS" per IP CAN Bearer: The PCEF is responsible for enforcing the policy-based authorization, that is to ensure that the requested QoS is in-line with the "Authorized QoS" per IP CAN Bearer.
- Policy Provisioning for Authorized QoS Per SDF: The provisioning of authorized QoS per SDF is a part of PCC rule provisioning procedure.
    - Policy Enforcement for Authorized QoS Per SDF: If an authorized QoS is defined for a PCC rule, the PCEF limits the data rate of the SDF corresponding to that PCC rule not to exceed the maximum authorized bandwidth for the PCC rule by discarding packets exceeding the limit.
    - Upon deactivation or removal of a PCC rule, the PCEF frees the resources reserved for that PCC rule. If the PCRF provides authorized QoS for both the IP-CAN bearer and PCC rule(s), the enforcement of authorized QoS of the individual PCC rules takes place first.

Important: In this release, coordination of authorized QoS scopes in mixed mode (BCM = UE_NW) is not supported.

    - Provisioning of Authorized QoS Per QCI: If the PCEF performs the bearer binding, the PCRF may provision an authorized QoS per QCI for non-GBR bearer QCI values. If the PCRF performs the bearer binding the PCRF does not provision an authorized QoS per QCI. The PCRF does not provision an authorized QoS per QCI for GBR bearer QCI values.
    - Policy Enforcement for Authorized QoS per QCI: The PCEF can receive an authorized QoS per QCI for non GBR-bearer QCI values.

- Other Features:
    - Bearer Control Mode Selection: The PCEF may indicate, via the Gx reference point, a request for Bearer Control Mode (BCM) selection at IP-CAN session establishment or IP-CAN session modification (as a consequence of an SGSN change). It will be done using the "PCC Rule Request" procedure.

      If the Bearer-Control-Mode AVP is not received from PCRF, the IP-CAN session is not terminated. The value negotiated between UE/SGSN/GGSN is considered as the BCM. The following values are considered for each of the service types:
        - GGSN: The negotiated value between UE/SGSN/GGSN is considered.

          In the following scenarios UE_ONLY is chosen as the BCM:

          Scenario 1:
            - UE-> UE_ONLY
            - SGSN-> UE_ONLY
            - GGSN-> UE_ONLY

- PCRF-> NO BCM

Scenario 2:

- UE-> UE_ONLY
- SGSN-> UE_ONLY
- GGSN-> Mixed
- PCRF-> NO BCM

- GTP-PGW: BCM of UE_NW is considered.
- IPSG: BCM of UE_ONLY is considered.
- HSGW/SGW/PDIF/FA/PDSN/HA/MIPV6HA: BCM of NONE is considered.

- PCC Rule Error Handling: If the installation/activation of one or more PCC rules fails, the PCEF includes one or more Charging-Rule-Report AVP(s) in either a CCR or an RAA command for the affected PCC rules. Within each Charging-Rule-Report AVP, the PCEF identifies the failed PCC rule(s) by including the Charging-Rule-Name AVP(s) or Charging-Rule-Base-Name AVP(s), identifies the failed reason code by including a Rule-Failure-Code AVP, and includes the PCC-Rule-Status AVP.

  If the installation/activation of one or more new PCC rules (that is, rules that were not previously successfully installed) fails, the PCEF sets the PCC-Rule-Status to INACTIVE for both the PUSH and the PULL modes.

  If a PCC rule was successfully installed/activated, but can no longer be enforced by the PCEF, the PCEF shall send the PCRF a new CCR command and include a Charging-Rule-Report AVP. The PCEF shall include the Rule-Failure-Code AVP within the Charging-Rule-Report AVP and shall set the PCC-Rule-Status to INACTIVE.

- Time of the Day Procedures: PCEF performs PCC rule request as instructed by the PCRF. Revalidation-Time when set by the PCRF, causes the PCEF to trigger a PCRF interaction to request PCC rules from the PCRF for an established IP CAN session. The PCEF stops the timer once the PCEF triggers a REVALIDATION_TIMEOUT event.

Important: In 11.0 and later releases Rule-Activation-Time / Rule-Deactivation-Time / Revalidation-Time AVP is successfully parsed only if its value corresponds to current time or a later time than the current IPSG time, else the AVP and entire message is rejected. In earlier releases the AVP is successfully parsed only if its value corresponds to a later time than the current IPSG time, else the AVP and entire message is rejected.

Charging Control

Charging Control is the process of associating packets belonging to a SDF to a charging key, and applying online charging and/or offline charging, as appropriate. Flow-based charging handles differentiated charging of the bearer usage based on real time analysis of the SDFs. In order to allow for charging control, the information in the PCC rule identifies the SDF and specifies the parameters for charging control. The PCC rule information may depend on subscription data.

In the case of online charging, it is possible to apply an online charging action upon PCEF events (for example, re-authorization upon QoS change).

It is possible to indicate to the PCEF that interactions with the charging systems are not required for a PCC rule, that is to perform neither accounting nor credit control for this SDF, and then no offline charging information is generated.

Supported Features:

- Provisioning of Charging-related Information for the IP-CAN Session.
- Provisioning of Charging Addresses: Primary or secondary event charging function name (Online Charging Server (OCS) addresses).

> ***Important:*** In this release, provisioning of primary or secondary charging collection function name (Offline Charging Server (OFCS) addresses) over Gx is not supported.

- Provisioning of Default Charging Method: In this release, the default charging method is sent in CCR-I message. For this, new AVPs Online/Offline are sent in CCR-I message based on the configuration.

Charging Correlation

For the purpose of charging correlation between SDF level and application level (for example, IMS) as well as on-line charging support at the application level, applicable charging identifiers and IP-CAN type identifiers are passed from the PCRF to the AF, if such identifiers are available.

For IMS bearer charging, the IP Multimedia Core Network (IM CN) subsystem and the Packet Switched (PS) domain entities are required to generate correlated charging data.

In order to achieve this, the Gateway provides the GGSN Charging Identifier (GCID) associated with the PDP context along with its address to the PCRF. The PCRF in turn sends the IMS Charging Identifier (ICID), which is provided by the P-CSCF, to the Gateway. The Gateway generates the charging records including the GCID as well as the ICID if received from PCRF, so that the correlation of charging data can be done with the billing system.

PCRF also provides the flow identifier, which uniquely identifies an IP flow in an IMS session.

Policy and Charging Control (PCC) Rules

A PCC rule enables the detection of an SDF and provides parameters for policy control and/or charging control. The purpose of the PCC rule is to:

- Detect a packet belonging to an SDF.
  - Select downlink IP CAN bearers based on SDF filters in the PCC rule.
  - Enforce uplink IP flows are transported in the correct IP CAN bearer using the SDF filters within the PCC rule.
- Identify the service that the SDF contributes to.
- Provide applicable charging parameters for an SDF.
- Provide policy control for an SDF.

The PCEF selects a PCC rule for each packet received by evaluating received packets against SDF filters of PCC rules in the order of precedence of the PCC rules. When a packet matches a SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied.

There are two types of PCC rules:

- Dynamic PCC Rules: Rules dynamically provisioned by the PCRF to the PCEF via the Gx interface. These PCC rules may be either predefined or dynamically generated in the PCRF. Dynamic PCC rules can be activated, modified, and deactivated at any time.
- Predefined PCC Rule: Rules preconfigured in the PCEF by the operators. Predefined PCC rules can be activated or deactivated by the PCRF at any time. Predefined PCC rules within the PCEF may be grouped allowing the PCRF to dynamically activate a set of PCC rules over the Gx reference point.

Important: A third type of rule, the static PCC rule can be preconfigured in the chassis by the operators. Static PCC rules are not explicitly known in the PCRF, and are not under control of the PCRF. Static PCC rules are bound to general purpose bearer with no Gx control.

A PCC rule consists of:

- Rule Name: The rule name is used to reference a PCC rule in the communication between the PCEF and PCRF.
- Service Identifier: The service identifier is used to identify the service or the service component the SDF relates to.
- Service Data Flow Filter(s): The service flow filter(s) is used to select the traffic for which the rule applies.
- Precedence: For different PCC rules with overlapping SDF filter, the precedence of the rule determines which of these rules is applicable. When a dynamic PCC rule and a predefined PCC rule have the same priority, the dynamic PCC rule takes precedence.
- Gate Status: The gate status indicates whether the SDF, detected by the SDF filter(s), may pass (gate is open) or will be discarded (gate is closed) in uplink and/or in downlink direction.
- QoS Parameters: The QoS information includes the QoS class identifier (authorized QoS class for the SDF), the Allocation and Retention Priority (ARP), and authorized bitrates for uplink and downlink.

  Important: In earlier releases, ECS used only the Priority-Level part of ARP byte for bearer binding, (along with QCI). Now the entire ARP byte is used for bearer binding (along with QCI). Since the capability and vulnerability bits are optional in a dynamic rule, if a dynamic rule is received without these flags, it is assumed that the capability bit is set to 1 (disabled) and vulnerability bit is set to 0 (enabled). For predefined rules, currently configuring these two flags is not supported, so as of now all predefined rules are assumed to have capability bit set to 1 (disabled) and vulnerability bit set to 0 (enabled).

- Charging key (rating group)
- Other charging parameters: The charging parameters define whether online and offline charging interfaces are used, what is to be metered in offline charging, on what level the PCEF will report the usage related to the rule, and so on.

Important: In this release, configuring the Metering Method and Reporting Level for dynamic PCC rules is not supported.

PCC rules also include Application Function (AF) record information for enabling charging correlation between the application and bearer layer if the AF has provided this information via the Rx interface. For IMS, this includes the IMS Charging Identifier (ICID) and flow identifiers.

PCC Procedures over Gx Reference Point

Request for PCC rules

The PCEF, via the Gx reference point, requests for PCC rules in the following instances:

- At IP-CAN session establishment.
- At IP-CAN session modification.

PCC rules can also be requested as a consequence of a failure in the PCC rule installation/activation or enforcement without requiring an event trigger.

Provisioning of PCC rules

The PCRF indicates, via the Rel. 7 Gx reference point, the PCC rules to be applied at the PCEF. This may be using one of the following procedures:

- PULL (provisioning solicited by the PCEF): In response to a request for PCC rules being made by the PCEF, the PCRF provisions PCC rules in the CC-Answer.
- PUSH (unsolicited provisioning): The PCRF may decide to provision PCC rules without obtaining a request from the PCEF. For example, in response to information provided to the PCRF via the Rx reference point, or in response to an internal trigger within the PCRF. To provision PCC rules without a request from the PCEF, the PCRF includes these PCC rules in an RA-Request message. No CCR/CCA messages are triggered by this RA-Request.

For each request from the PCEF or upon unsolicited provision the PCRF provisions zero or more PCC rules. The PCRF may perform an operation on a single PCC rule by one of the following means:

- To activate or deactivate a PCC rule that is predefined at the PCEF, the PCRF provisions a reference to this PCC rule within a Charging-Rule-Name AVP and indicates the required action by choosing either the Charging-Rule-Install AVP or the Charging-Rule-Remove AVP.
- To install or modify a PCRF-provisioned PCC rule, the PCRF provisions a corresponding Charging-Rule-Definition AVP within a Charging-Rule-Install AVP.
- To remove a PCC rule which has previously been provisioned by the PCRF, the PCRF provisions the name of this rule as value of a Charging-Rule-Name AVP within a Charging-Rule-Remove AVP.
- If the PCRF performs the bearer binding, the PCRF may move previously installed or activated PCC rules from one IP CAN bearer to another IP CAN bearer.

Important: In 11.0 and later releases, the maximum valid length for a charging rule name is 63 bytes. When the length of the charging rule name is greater than 63 bytes, a charging rule report with RESOURCES_LIMITATION as Rule-Failure-Code is sent. This charging rule report is sent only when the length of the rule name is lesser than 128 characters. When the charging rule name length is greater than or equal to 128 characters no charging rule report will be sent. In earlier releases, the length of the charging rule name constructed by PCRF was limited to 32 bytes.

Selecting a PCC Rule for Uplink IP Packets

If PCC is enabled, the PCEF selects the applicable PCC rule for each received uplink IP packet within an IP CAN bearer by evaluating the packet against uplink SDF filters of PCRF-provided or predefined active PCC rules of this IP CAN bearer in the order of the precedence of the PCC rules.

Important: When a PCRF-provided PCC rule and a predefined PCC rule have the same precedence, the uplink SDF filters of the PCRF-provided PCC rule is applied first.

Important: In 11.0 and later releases, IMSA and ECS allow the PCRF to install two (or more) dynamic rules with the same precedence value. In earlier releases, for two distinct dynamic rules having the same precedence the second rule used to be rejected.

When a packet matches an SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied. Uplink IP packets which do not match any PCC rule of the corresponding IP CAN bearer are discarded.

Selecting a PCC Rule and IP CAN Bearer for Downlink IP Packets

If PCC is enabled, the PCEF selects a PCC rule for each received downlink IP packet within an IP CAN session by evaluating the packet against downlink SDF filters of PCRF-provided or predefined active PCC rules of all IP CAN bearers of the IP CAN session in the order of the precedence of the PCC rules.

Important: When a PCRF-provided PCC rule and a predefined PCC rule have the same precedence, the downlink SDF filters of the PCRF-provided PCC rule are applied first.

When a packet matches a SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied. The Downlink IP Packet is transported within the IP CAN bearer where the selected PCC rule is mapped. Downlink IP packets that do not match any PCC rule of the IP CAN session are discarded.

The following procedures are also supported:

- Indication of IP-CAN Bearer Termination Implications
- Indication of IP-CAN Session Termination: When the IP-CAN session is being terminated (for example, for GPRS when the last PDP Context within the IP-CAN session is being terminated) the PCEF contacts the PCRF.
- Request of IP-CAN Bearer Termination: If the termination of the last IP CAN bearer within an IP CAN session is requested, the PCRF and PCEF apply the “Request of IP-CAN Session Termination” procedure.
- Request of IP-CAN Session Termination: If the PCRF decides to terminate an IP CAN session due to an internal trigger or trigger from the SPR, the PCRF informs the PCEF. The PCEF acknowledges to the PCRF and instantly removes/deactivates all the PCC rules that have been previously installed or activated on that IP-CAN session.

The PCEF applies IP CAN specific procedures to terminate the IP CAN session. For GPRS, the GGSN send a PDP context deactivation request with the teardown indicator set to indicate that the termination of the entire IP-CAN session is requested. Furthermore, the PCEF applies the “Indication of IP CAN Session Termination” procedure.

In 12.0 and later releases, volume or rule information obtained from PCRF is discarded if the subscriber is going down.

Volume Reporting Over Gx

This section describes the 3GPP Rel. 9 Volume Reporting over Gx feature, which is supported by all products supporting Rel. 7 Gx interface.

License Requirement

The Volume Reporting over Gx feature requires the following license to be installed on the chassis:

Cisco PID [ASR5K-00-CS01CHGX] *Charging Over Gx, 1K sessions*, or Starent Part Number [600-00-7822] *Charging Over Gx*.

For information on obtaining and installing licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *Cisco ASR 5000 Series System Administration Guide*.

Supported Standards

The Volume Reporting over Gx feature is based on the following standard:

3GPP TS 29.212 V9.3.0 (2010-06): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 9).

Feature Overview

The Volume Reporting over Gx feature provides PCRF the capability to make real-time decisions based on the data usage by subscribers.

Important: Volume Reporting over Gx is applicable only for volume quota.

Important: In release 10.0, only total data usage reporting is supported, uplink/downlink level reporting is not supported. In 10.2 and later releases, it is supported.

Important: The PCEF only reports the accumulated usage since the last report for usage monitoring and not from the beginning.

Important: If the usage threshold is set to zero (infinite threshold), no further threshold events will be generated by PCEF, but monitoring of usage will continue and be reported at the end of the session.

The following steps explain how Volume Reporting over Gx works:

1. PCEF after receiving the message from PCRF parses the usage monitoring related AVPs, and sends the information to IMSA.
2. IMSA updates the information to ECS.
3. Once the ECS is updated with the usage monitoring information from PCRF, the PCEF (ECS) starts tracking the data usage.
4. For session-level monitoring, the ECS maintains the amount of data usage.

5. For PCC rule monitoring, usage is monitored with the monitoring key as the unique identifier. Each node maintains the usage information per monitoring key. When the data traffic is passed, the usage is checked against the usage threshold values and reported as described in the *Usage Reporting* section.
6. The PCEF continues to track data usage after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session.

Usage Monitoring

- Usage Monitoring at Session Level: PCRF subscribes to the session-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to SESSION_LEVEL(0). After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. In 11.0 and later releases, Monitoring Key at session level is supported.

  In 12.0 and later releases, enabling and disabling session usage in a single message from PCRF is supported. This is supported only if the monitoring key is associated at session level.

  In 12.0 and later releases, monitoring of usage based on input/output octet threshold levels is supported. Usage is reported based on the enabled threshold level. If multiple levels are enabled, usage will be reported on all the enabled levels even if only one of the levels is breached. Monitoring will be stopped on the missing threshold levels in the response for the usage report from PCRF (expected to provide the complete set again if PCRF wants to continue monitoring on the multiple levels enabled earlier).

  Total threshold level along with UL/DL threshold level in the GSU AVP is treated as an error and only total threshold level is accepted.
- Usage Monitoring at Flow Level: PCRF subscribes to the flow-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to PCC_RULE_LEVEL(1). Monitoring Key is mandatory in case of a flow-level monitoring since the rules are associated with the monitoring key and enabling/disabling of usage monitoring at flow level can be controlled by PCRF using it. After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

  Usage monitoring is supported for static, predefined rules, and dynamic rule definitions.

  - Usage Monitoring for Static Rules: In the case of static rules, the usage reporting on last rule removal associated with the monitoring key is not applicable. In this case only the usage monitoring information is received from the PCRF.
  - Usage Monitoring for Predefined Rules: If the usage monitoring needs to be enabled for the predefined rules, PCRF sends the rule and the usage monitoring information containing the monitoring key and the usage threshold. The Monitoring key should be same as the one pre-configured in PCEF for that predefined rule. There can be multiple rules associated with the same monitoring key. Hence enabling a particular monitoring key would result in the data being tracked for multiple rules having the same monitoring key. After DPCA parses the AVPs IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.
  - Usage Monitoring for Dynamic Rules: If the usage monitoring needs to be enabled for dynamic ruledefs, PCRF provides the monitoring key along with a charging rule definition and the usage

monitoring information containing the monitoring key and the usage threshold. This would result in the usage monitoring being done for all the rules associated with that monitoring key. After DPCA parses the AVPs, IMSA updates the information to ECS. Once ECS is updated, the usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. Monitoring key for dynamic ruledef is dynamically assigned by PCRF which is the only difference with predefined rules in case of usage monitoring.

Usage Reporting

Usage at subscriber/flow level is reported to PCRF under the following conditions:

- Usage Threshold Reached: PCEF records the subscriber data usage and checks if the usage threshold provided by PCRF is reached. This is done for both session and rule level reporting.

  For session-level reporting, the actual usage volume is compared with the usage volume threshold.

  For rule-level reporting the rule that hits the data traffic is used to find out if the monitoring key is associated with it, and based on the monitoring key the data usage is checked. Once the condition is met, it reports the usage information to IMSA and continues monitoring. IMSA then triggers the CCR-U if "USAGE_REPORT" trigger is enabled by the PCRF. The Usage-Monitoring-Information AVP is sent in this CCR with the "Used-Service-Unit" set to the amount of data usage by subscriber.

  If PCRF does not provide a new usage threshold in the usage monitoring information as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no usage status is reported.

  In the non-standard Volume Reporting over Gx implementation, usage monitoring will be stopped once the threshold is breached, else the monitoring will continue. There will be no further usage reporting until the CCA is received.
- Usage Monitoring Disabled: If the PCRF explicitly disables the usage monitoring with Usage-Monitoring-Support AVP set to USAGE_MONITORING_DISABLED, the PCEF stops monitoring and reports the usage information (when the monitoring was enabled) to PCRF if the usage monitoring is disabled by PCRF as a result of CCR from PCEF which is not related to reporting usage, other external triggers, or a PCRF internal trigger. If the PCRF does not provide a new usage threshold as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no further usage status is reported.
- IP CAN Session Termination: When the IP CAN session is terminated, the accumulated subscriber usage information is reported to PCRF in the CCR-T from PCEF. If PCC usage level information is enabled by PCRF, the PCC usage will also be reported.
- PCC Rule Removal: When the PCRF deactivates the last PCC rule associated with a usage monitoring key, the PCEF sends a CCR with the data usage for that monitoring key. If the PCEF reports the last PCC rule associated with a usage monitoring key is inactive, the PCEF reports the accumulated usage for that monitoring key within the same CCR command if the Charging-Rule-Report AVP was included in a CCR command; otherwise, if the Charging-Rule-Report AVP was included in an RAA command, the PCEF sends a new CCR command to report accumulated usage for the usage monitoring key. In 12.0 and later releases, usage reporting on last rule deactivation using rule deactivation time set by PCRF is supported.
- PCRF Requested Usage Report: In 10.2 and later releases, the accumulated usage since the last report is sent even in case of immediate reporting, the usage is reset after immediate reporting and usage monitoring continued so that the subsequent usage report will have the usage since the current report. In earlier releases the behavior was to accumulate the so far usage in the next report.
- Revalidation Timeout: In the non-standard implementation, if usage monitoring and reporting is enabled and a revalidation timeout occurs, the PCEF sends a CCR to request PCC rules and reports all accumulated usage for

all enabled monitoring keys since the last report (or since usage reporting was enabled if the usage was not yet reported) with the accumulated usage at IP-CAN session level (if enabled) and at service data flow level (if enabled) This is the default behavior.

In the case of standard implementation, this must be enabled by CLI configuration.

Important: The Usage Reporting on Revalidation Timeout feature is available by default in non-standard implementation of Volume Reporting over Gx. In 10.2 and later releases, this is configurable in the standard implementation. This is not supported in 10.0 release for standard based volume reporting.

Once the usage is reported, the usage counter is reset to zero. The PCEF continues to track data usage from the zero value after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session and and the usage accumulated between the CCR-CCA will be discarded.

For information on how to configure the Volume Reporting over Gx feature, see the Configuring Volume Reporting over Gx section.

How Rel. 7 Gx Works

This section describes how dynamic policy and charging control for subscribers works with Rel. 7 Gx interface support in GPRS/UMTS networks.

The following figure and table explain the IMSA process between a system and IMS components that is initiated by the UE.

In this example, the Diameter Policy Control Application (DPCA) is the Gx interface to the PCRF. The interface between IMSA with PCRF is the Gx interface, and the interface between Session Manager (SessMgr) and Online Charging Service (OCS) is the Gy interface. Note that the IMSA service and DPCA are part of SessMgr on the system and separated in the figure for illustration purpose only.

Figure 10. Rel. 7 Gx IMS Authorization Call Flow

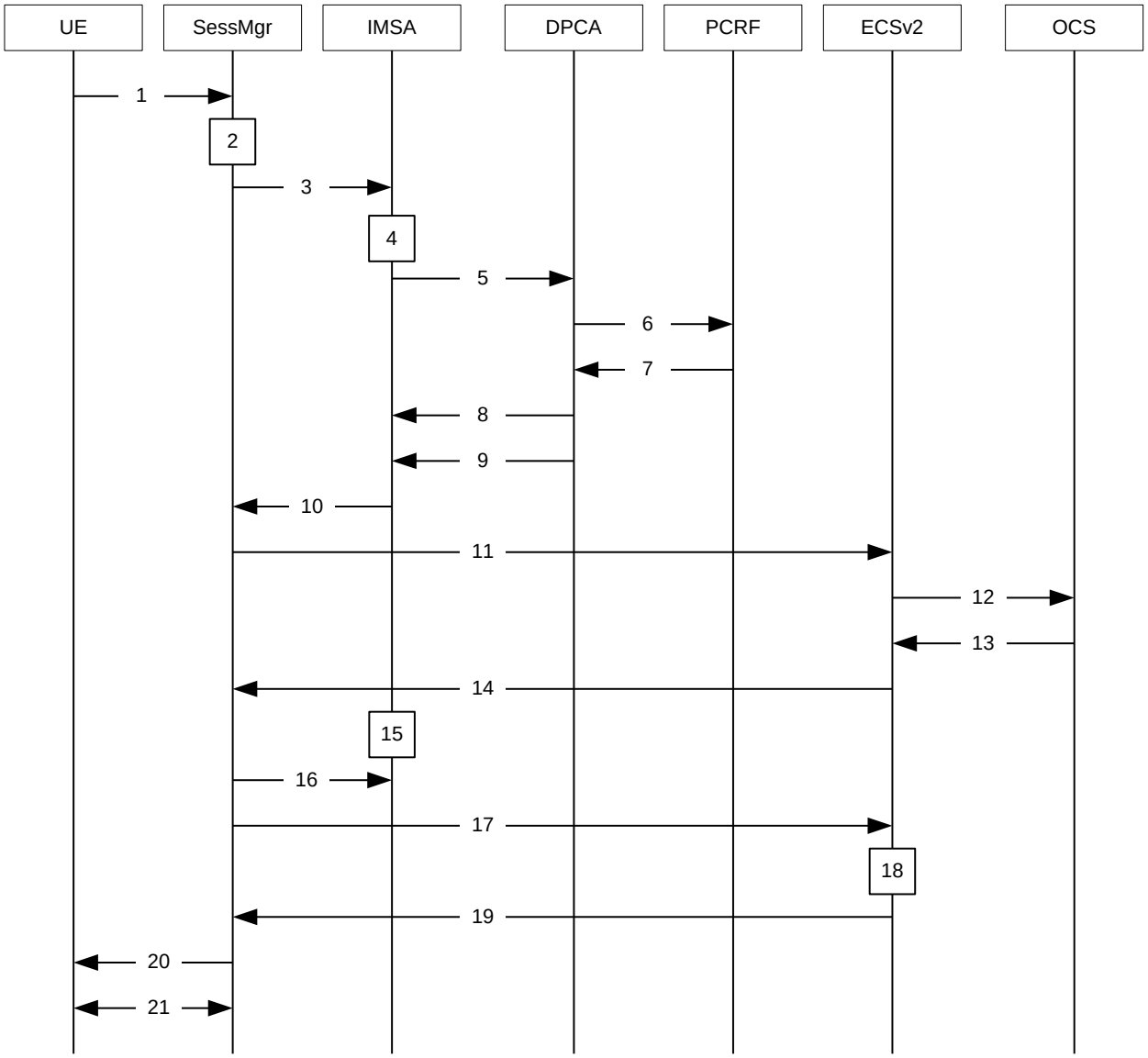


Table 3. Rel. 7 Gx IMS Authorization Call flow Description

Step	Description
1	UE (IMS subscriber) requests for primary PDP context activation/creation.
2	SessMgr allocates an IP address to the UE.
3	SessMgr requests IMS Authorization, if IMSA is enabled for the APN.
4	IMSA allocates resources for the IP CAN session and the bearer, and selects the PCRF to contact based on the user's selection key (for example, msisdn).
5	IMSA requests the DPCA module to issue an auth request to the PCRF.

Step	Description
6	DPCA sends a CCR initial message to the selected PCRF. This message includes the Context-Type AVP set to PRIMARY and the IP address allocated to the UE. The message may include the Bearer-Usage AVP set to GENERAL. The Bearer-Operation is set to Establishment. The Bearer ID is included if the PCRF does the bearer binding.
7	PCRF may send preconfigured charging rules in CCA, if a preconfigured rule set for general purpose PDP context is provided in PCRF. The dynamic rules and the authorized QoS parameters could also be included by the PCRF.
8	DPCA passes the charging rule definition, charging rule install, QoS information received from the PCRF, event triggers, and so on, along with the Bearer ID that corresponds to the rules received from the PCRF to IMSA. IMSA stores the information. If the Bearer ID is absent, and PCRF does the bearer binding, the rule is skipped. Whereas, if the Bearer ID is absent and the PCEF does the bearer binding, the rule is passed onto the ECS to perform bearer binding.
9	DPCA calls the callback function registered with it by IMSA.
10	IMSA stores the bearer authorized QoS information and notifies the SessMgr. Other PCRF provided information common to the entire PDP session (event trigger, primary/secondary OCS address, and so on) is stored within the IMSA. After processing the information, IMSA notifies the SessMgr about the policy authorization complete.
11	If the validation of the rules fails in IMSA/DPCA, a failure is notified to PCRF containing the Charging-Rule-Report AVP. Else, IMSA initiates creation of ECS session. The APN name, primary/secondary OCS server address, and so on are sent to the ECS from the SessMgr.
12	ECS performs credit authorization by sending CCR(I) to OCS with CC-Request-Type set to INITIAL_REQUEST to open the credit control session. This request includes the active Rulebase-Id (default rulebase ID from the APN/AAA) and GPRS specific attributes (for example, APN, UMTS QoS, and so on).
13	OCS returns a CCA initial message that may activate a statically configured Rulebase and may include preemptive quotas.
14	ECS responds to SessMgr with the response message.
15	SessMgr requests IMSA for the dynamic rules.
16	IMSA sends the dynamic rules to SessMgr. Note that until the primary PDP context is established, all RAR messages from the PCRF are rejected.
17	SessMgr sends the dynamic rule information to the ECS. The gate flow status information and the QoS per flow (charging rule) information are also sent in the message.
18	ECS activates the predefined rules received, and installs the dynamic rules received. Also, the gate flow status and the QoS parameters are updated by ECS as per the dynamic charging rules. The Gx rulebase is treated as an ECS group-of-ruledefs. The response message contains the Charging Rule Report conveying the status of the rule provisioning at the ECS. ECS performs PCEF bearer binding for rules without bearer ID.
19	If the provisioning of rules fails partially, the context setup is accepted, and a new CCR-U is sent to the PCRF with the Charging-Rule-Report containing the PCC rule status for the failed rules. If the provisioning of rules fails completely, the context setup is rejected.
20	Depending on the response for the PDP Context Authorization, SessMgr sends the response to the UE and activates/rejects the call. If the Charging-Rule-Report contains partial failure for any of the rules, the PCRF is notified, and the call is activated. If the Charging-Rule-Report contains complete failure, the call is rejected.
21	Based on the PCEF bearer binding for the PCC rules at Step 18, the outcome could be one or more network-initiated PDP context procedures with the UE (Network Requested Update PDP Context (NRUPC) / Network Requested Secondary PDP Context Activation (NRSPCA)).

Configuring Rel. 7 Gx Interface

To configure Rel. 7 Gx interface functionality, the IMS Authorization service must be configured at the context level, and then the APN configured to use the IMS Authorization service.

To configure Rel. 7 Gx interface functionality:

Step 1 Configure IMS Authorization service at the context level for IMS subscriber in GPRS/UMTS network as described in the Configuring IMS Authorization Service at Context Level section.

Step 2 Verify your configuration as described in the Verifying the Configuration section.

Step 3 Configure an APN within the same context to use the IMS Authorization service for IMS subscriber as described in the Applying IMS Authorization Service to an APN section.

Step 4 Verify your configuration as described in the Verifying Subscriber Configuration section.

Step 5 *Optional:* Configure the Volume Reporting over Gx feature as described in the Configuring Volume Reporting over Gx section.

Step 6 Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Important: Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Cisco ASR 5000 Series Command Line Interface Reference* for complete information regarding all commands.

Configuring IMS Authorization Service at Context Level

Use the following example to configure IMS Authorization service at context level for IMS subscribers in GPRS/UMTS networks:

```
configure
   context <context_name>
      ims-auth-service <imsa_service_name>
         p-cscf discovery table { 1 | 2 } algorithm { ip-address-modulus |
msisdn-modulus | round-robin }
         p-cscf table { 1 | 2 } row-precedence <precedence_value> { address
<ip_address> | ipv6-address <ipv6_address> } [ secondary { address <ip_address>
| ipv6-address <ipv6_address> } ]
         policy-control
            diameter origin endpoint <endpoint_name>
            diameter dictionary <dictionary>
```

```
diameter request-timeout <timeout_duration>

diameter host-select table { { { 1 | 2 } algorithm { ip-address-
modulus | msisdn-modulus | round-robin } } | prefix-table { 1 | 2 } }

diameter host-select row-precedence <precedence_value> table { { { 1
| 2 } host <host_name> [ realm <realm_id> ] [ secondary host <host_name> [ realm
<realm_id> ] ] } | { prefix-table { 1 | 2 } msisdn-prefix-from
<msisdn_prefix_from> msisdn-prefix-to <msisdn_prefix_to> host <host_name> [
realm <realm_id> ] [ secondary host <sec_host_name> [ realm <sec_realm_id> ]
algorithm { active-standby | round-robin } ] } } [ -noconfirm ]

diameter host-select reselect subscriber-limit <subscriber_limit>
time-interval <duration>

failure-handling cc-request-type { any-request | initial-request |
terminate-request | update-request } { diameter-result-code { any-error |
<result_code> [ to <end_result_code> ] } } { continue | retry-and-terminate |
terminate }

end
```

Notes:

- <*context_name*> must be the name of the context where you want to enable IMS Authorization service.
- <*imsa_service_name*> must be the name of the IMS Authorization service to be configured for Rel. 7 Gx interface authentication.
- A maximum of 16 authorization services can be configured globally in a system. There is also a system limit for the maximum number of total configured services.
- To enable Rel. 7 Gx interface support, pertinent Diameter dictionary must be configured. For information on the specific Diameter dictionary to use, please contact your local service representative.
- When configuring the MSISDN prefix range based PCRF selection mechanism:

  To enable the Gx interface to connect to a specific PCRF for a range of subscribers configure **msisdn-prefix-from** <*msisdn_prefix_from*> and **msisdn-prefix-to** <*msisdn_prefix_to*> with the starting and ending MSISDNs respectively.

  To enable the Gx interface to connect to a specific PCRF for a specific subscriber, configure both **msisdn-prefix-from** <*msisdn_prefix_from*> and **msisdn-prefix-to** <*msisdn_prefix_to*> with the same MSISDN.

  In StarOS 8.1 and later releases, per MSISDN prefix range table a maximum of 128 rows can be added. In StarOS 8.0 and earlier releases, a maximum of 100 rows can be added.

  The MSISDN ranges must not overlap between rows.
- The Round Robin algorithm for PCRF selection is effective only over a large number of PCRF selections, and not at a granular level.
- *Optional:* To configure the Quality of Service (QoS) update timeout for a subscriber, in the IMS Authorization Service Configuration Mode, enter the following command:

  qos-update-timeout <*timeout_duration*>

- *Optional:* To configure signalling restrictions, in the IMS Authorization Service Configuration Mode, enter the following commands:

  signaling-flag { deny | permit }

  signaling-flow permit server-address <*ip_address*> **[server-port {** <*port_number*> **| range** <*start_number*> **to** <*end_number*> **}] [description** <*string*> **]**

- *Optional*: To configure action on packets that do not match any policy gates in the general purpose PDP context, in the IMS Authorization Service Configuration Mode, enter the following command:

  traffic-policy general-pdp-context no-matching-gates direction { downlink | uplink } { forward | discard }

- To configure the PCRF host destinations configured in the GGSN/PCEF, use the **diameter host-select** CLI commands.
- To configure the GGSN/PCEF to use a pre-defined rule when the Gx fails, set the **failure-handling cc-request-type** CLI to **continue**. Policies available/in use will continue to be used and there will be no further interaction with the PCRF.
- For provisioning of default charging method, use the following configurations. For this, the AVPs Online and Offline will be sent in CCR-I message based on the configuration.
  - To send Enable Online:

    ```
    configure
       active-charging service <ecs_service_name>
          charging-action <charging_action_name>
             cca charging credit
             exit
    ```

  - To send Enable Offline:

    ```
    configure
       active-charging service <ecs_service_name>
          rulebase <rulebase_name>
             billing-records rf
             exit
    ```

Verifying the Configuration

To verify the IMS Authorization service configuration:

Step 1 Change to the context where you enabled IMS Authorization service by entering the following command:

```
context <context_name>
```

Step 2 Verify the IMS Authorization service's configurations by entering the following command:

```
show ims-authorization service name <imsa_service_name>
```

Applying IMS Authorization Service to an APN

After configuring IMS Authorization service at the context-level, an APN within the same context must be configured to use the IMS Authorization service for an IMS subscriber.

Use the following example to apply IMS Authorization service functionality to a previously configured APN within the context configured in the Configuring Rel. 7 Gx Interface section.

```
configure
   context <context_name>
      apn <apn_name>
         ims-auth-service <imsa_service_name>
         active-charging rulebase <rulebase_name>
         end
```

Notes:

- *<context_name>* must be the name of the context in which the IMS Authorization service was configured.
- *<imsa_service_name>* must be the name of the IMS Authorization service configured for IMS authentication in the context.
- For Rel. 7 Gx, the ECS rulebase must be configured in the APN.
- ECS allows change of rulebase via Gx for PCEF binding scenarios. When the old rulebase goes away, all the rules that were installed from that rulebase are removed. This may lead to termination of a few bearers (PDP contexts) if they are left without any rules. If there is a Gx message that changes the rulebase, and also activates some predefined rules, the rulebase change is made first, and the rules are activated from the new rulebase. Also, the rulebase applies to the entire call. All PDP contexts (bearers) in one call use the same ECS rulebase.
- For predefined rules configured in the ECS, MBR/GBR of a dynamic/predefined rule is checked before it is used for PCEF binding. All rules (dynamic as well as predefined) have to have an MBR associated with them and all rules with GBR QCI should have GBR also configured. So for predefined rules, one needs to configure appropriate peak-data-rate, committed-data-rate as per the QCI being GBR QCI or non-GBR QCI. For more information, in the ACS Charging Action Configuration Mode, see the **flow limit-for-bandwidth** CLI command.
- Provided interpretation of the Gx rulebase is chosen to be ECS group-of-ruledefs, in the Active Charging Service Configuration Mode configure the following command:

  policy-control charging-rule-base-name active-charging-group-of-ruledefs

Verifying Subscriber Configuration

Verify the IMS Authorization service configuration for subscriber(s) by entering the following command:

show subscribers ims-auth-service *<imsa_service_name>*

<imsa_service_name> must be the name of the IMS Authorization service configured for IMS authentication.

Configuring Volume Reporting over Gx

This section describes the configuration required to enable Volume Reporting over Gx.

To enable Volume Reporting over Gx, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      rulebase <rulebase_name>
         action priority <priority> dynamic-only ruledef <ruledef_name>
charging-action <charging_action_name> monitoring-key <monitoring_key>
         exit
      exit
   context <context_name>
      ims-auth-service <imsa_service_name>
         policy-control
            event-update send-usage-report [ reset-usage ]
            end
```

Notes:

- The maximum accepted monitoring key value by the PCEF is 4294967295. If the PCEF sends a greater value, the value is converted to an Unsigned Integer value.
- The **event-update** CLI which enables volume usage report to be sent in event updates is available only in 10.2 and later releases. The optional keyword **reset-usage** enables to support delta reporting wherein the usage is reported and reset at PCEF. If this option is not configured, the behavior is to send the usage information as part of event update but not reset at PCEF.

Gathering Statistics

This section explains how to gather Rel. 7 Gx statistics and configuration information.

In the following table, the first column lists what statistics to gather, and the second column lists the action to perform.

Table 4. Gathering Rel. 7 Gx Statistics and Information

Statistics/Information	Action to perform
Information and statistics specific to policy control in IMS Authorization service.	**show ims-authorization policy-control statistics**
Information and statistics specific to the authorization servers used for IMS Authorization service.	**show ims-authorization servers ims-auth-service**
Information of all IMS Authorization service.	**show ims-authorization service all**
Statistics of IMS Authorization service.	**show ims-authorization service statistics**
Information, configuration, and statistics of sessions active in IMS Authorization service.	**show ims-authorization sessions all**
Complete information, configuration, and statistics of sessions active in IMS Authorization service.	**show ims-authorization sessions full**
Summarized information of sessions active in IMS Authorization service.	**show ims-authorization sessions summary**
Complete statistics for active charging service sessions.	**show active-charging sessions full**
Information for all rule definitions configured in the service.	**show active-charging ruledef all**
Information for all rulebases configured in the system.	**show active-charging rulebase all**
Information on all group of ruledefs configured in the system.	**show active-charging group-of-ruledefs all**
Information on policy gate counters and status.	**show ims-authorization policy-gate { counters | status }**

Rel. 8 Gx Interface

Rel. 8 Gx interface support is available on the Cisco ASR 5000 platform running StarOS 10.0 or StarOS 11.0 and later releases.

This section describes the following topics:

HA/PDSN Rel. 8 Gx Interface Support

This section provides information on configuring Rel. 8 Gx interface for HA and PDSN to support policy and charging control for subscribers in CDMA networks.

The IMS service provides application support for transport of voice, video, and data independent of access support. Roaming IMS subscribers in CDMA networks require apart from other functionality sufficient, uninterrupted, consistent, and seamless user experience during an application session. It is also important that a subscriber gets charged only for the resources consumed by the particular IMS application used.

It is recommended that before using the procedures in this section you select the configuration example that best meets your service model, and configure the required elements for that model as described in this Administration Guide.

This section describes the following topics:

Introduction

For IMS deployment in CDMA networks the system uses Rel. 8 Gx interface for policy-based admission control support and flow-based charging (FBC). The Rel. 8 Gx interface supports enforcing policy control features like gating, bandwidth limiting, and so on, and also supports FBC. This is accomplished via dynamically provisioned Policy Control and Charging (PCC) rules. These PCC rules are used to identify Service Data Flows (SDF) and to do charging. Other parameters associated with the rules are used to enforce policy control.

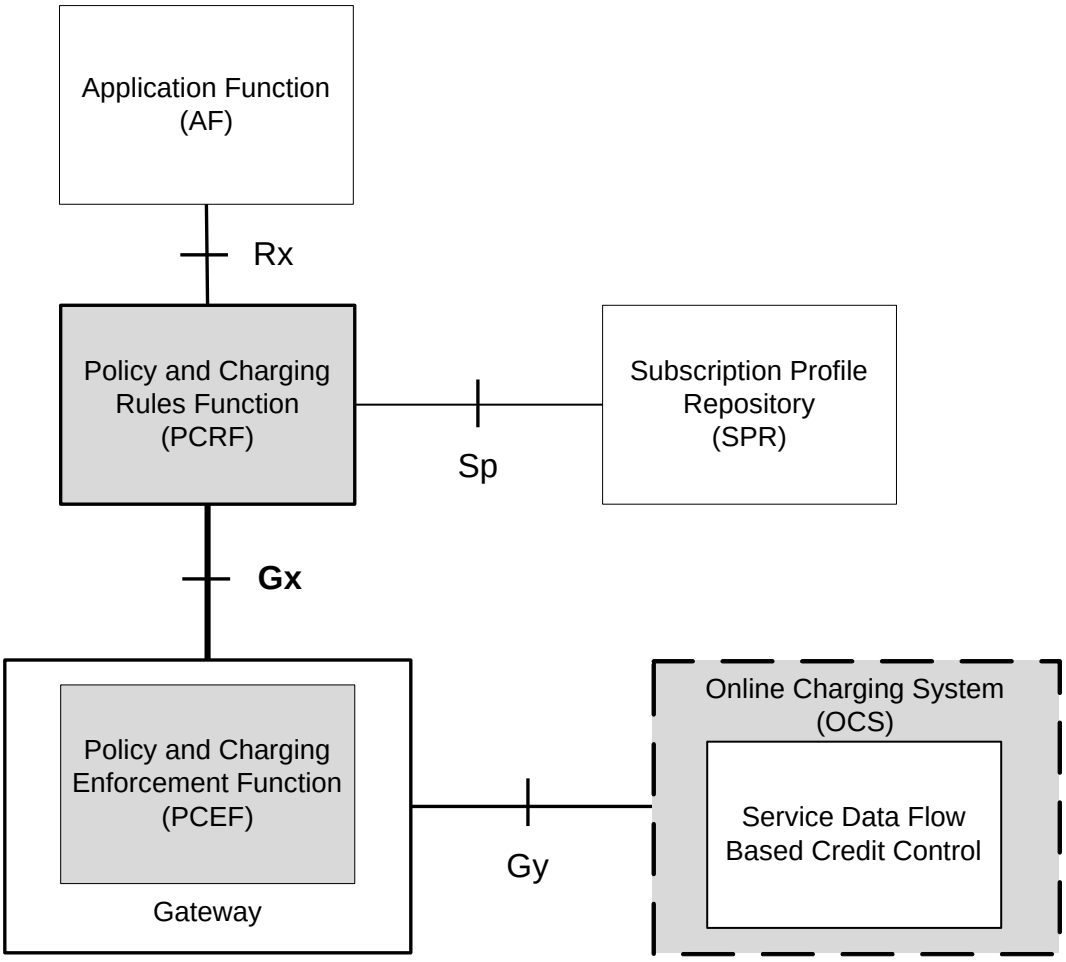
The PCC architecture allows operators to perform service-based QoS policy and FBC control. In the PCC architecture, this is accomplished mainly by the Policy and Charging Enforcement Function (PCEF)/HA/PDSN and the Policy and

Charging Rules Function (PCRF). The client functionality lies with the HA/PDSN, therefore in the IMS Authorization (IMSA) scenario it is also called the Gateway. The PCEF function is provided by the Enhanced Charging Service (ECS). The Gx interface is implemented as a Diameter connection. The Gx messaging mostly involves installing/modifying/removing dynamic rules and activating/deactivating predefined rules.

The Gx reference point is located between the Gateway/PCEF and the PCRF. This reference point is used for provisioning and removal of PCC rules from the PCRF to the Gateway/PCEF, and the transmission of traffic plane events from the Gateway/PCEF to the PCRF. The Gx reference point can be used for charging control, policy control, or both by applying AVPs relevant to the application.

The following figure shows the reference points between elements involved in the policy and charging architecture.

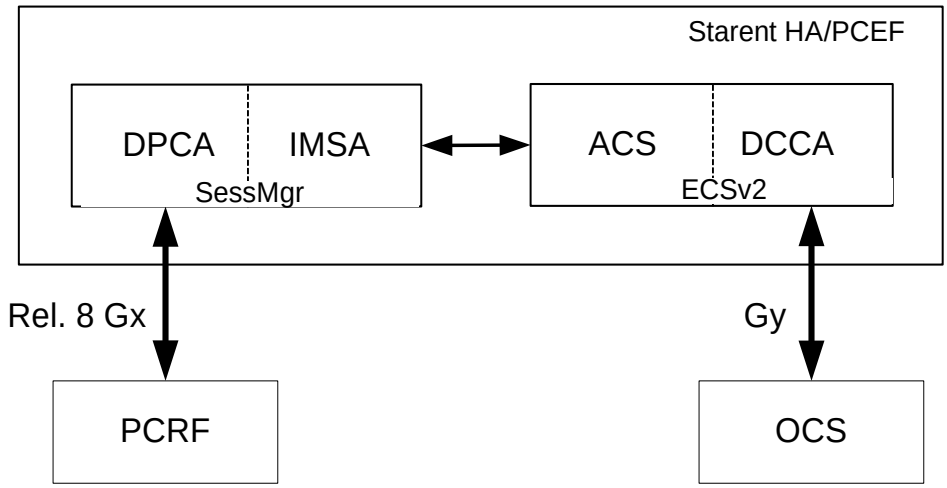
Figure 11. HA/PDSN Rel. 8 Gx PCC Logical Architecture



Within the Gateway, the IMSA and DPCA modules handle the Gx protocol related functions (at the SessMgr) and the policy enforcement and charging happens at ECS. The Gy protocol related functions are handled within the DCCA module (at the ECS).

The following figure shows the interaction between components within the Gateway.

Figure 12. HA/PDSN Rel. 8 Gx PCC Architecture within PCEF



Licensing

HA/PDSN Rel. 8 Gx interface requires the following licenses to be installed on the chassis:

- Cisco PID [ASR5K-00-CS01PIF] *Policy Interface, 1K sessions*, or Starent Part Number [600-00-7585] *Dynamic Policy Interface* — license for IMS Authorization Service feature.
- Cisco PID [ASR5K-00-CS01ECG2] *Enhanced Charging Bundle 2 1k Sessions*, or Starent Part Number [600-00-7574] *Enhanced Charging Bundle 2 1k Sessions* — To enable and configure Diameter and ECS functionality.

Supported Standards

HA/PDSN Rel 8. Gx interface support is based on the following standards and RFCs:

- 3GPP TS 23.203 V8.3.0 (2008-09) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 8)
- 3GPP TS 29.212 V8.6.0 (2009-12) 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 8)
- 3GPP TS 29.213 V8.1.1 (2008-10) 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control signalling flows and QoS parameter mapping; (Release 8)
- RFC 3588, Diameter Base Protocol; September 2003
- RFC 4006, Diameter Credit-Control Application; August 2005

Terminology and Definitions

This section describes features and terminology pertaining to HA/PDSN Rel. 8 Gx functionality.

Policy Control

The process whereby the PCRF indicates to the PCEF how to control the IP-CAN session.

Policy control comprises the following functions:

- Binding
- Gating Control
- Event Reporting
- QoS Control
- Other Features

Binding

In the HA/PDSN Rel. 8 Gx implementation, since there are no bearers within a MIP session the IP-CAN Bearer concept does not apply. Only authorized IP-CAN session is applicable.

Gating Control

Gating control is the blocking or allowing of packets belonging to an SDF, to pass through to the desired endpoint. A gate is described within a PCC rule and gating control is applied on a per SDF basis. The commands to open or close the gate leads to the enabling or disabling of the passage for corresponding IP packets. If the gate is closed, all packets of the related IP flows are dropped. If the gate is open, the packets of the related IP flows are allowed to be forwarded.

Event Reporting

Important: Unconditional reporting of event triggers from PCRF to PCEF when PCEF has not requested for is not supported.

Important: In the HA/PDSN Rel. 8 Gx implementation, only the AN_GW_CHANGE (21) event trigger is supported.

Event reporting is the notification of and reaction to application events to trigger new behavior in the user plane as well as the reporting of events related to the resources in the Gateway (PCEF). Event triggers may be used to determine which IP-CAN session modification or specific event causes the PCEF to re-request PCC rules. Event trigger reporting from PCEF to PCRF, and provisioning of event triggers happens at IP-CAN session level.

The Event Reporting Function (ERF) located in the PCEF, receives event triggers from PCRF during the Provision of PCC Rules procedure and performs event trigger detection. When an event matching the received event trigger occurs, the ERF reports the occurred event to the PCRF. If the provided event triggers are associated with certain parameter values then the ERF includes those values in the response to the PCRF.

QoS Control

Important: In the HA/PDSN Rel. 8 Gx implementation, only authorized IP-CAN Session is supported. Provisioning of authorized QoS per IP-CAN bearer, policy enforcement for authorized QoS per QCI, and coordination of authorized QoS scopes in mixed mode are not applicable.

QoS control is the authorization and enforcement of the maximum QoS that is authorized for an SDF. In case of an aggregation of multiple SDFs, the combination of the authorized QoS information of the individual SDFs is provided as the authorized QoS for this aggregate. QoS control per SDF allows the PCC architecture to provide the PCEF with the authorized QoS to be enforced for each specific SDF.

QoS authorization information may be dynamically provisioned by the PCRF, or it can be a predefined PCC rule in the PCEF. For a predefined PCC rule within the PCEF, the authorized QoS information takes affect when the PCC rule is activated. The PCEF combines the different sets of authorized QoS information, that is the information received from the PCRF and the information corresponding to the predefined PCC rules. The PCRF knows the authorized QoS information of the predefined PCC rules and takes this information into account when activating them. This ensures that the combined authorized QoS of a set of PCC rules that are activated by the PCRF is within the limitations given by the subscription and operator policies regardless of whether these PCC rules are dynamically provided, predefined, or both.

Supported features include:

- Provisioning and Policy Enforcement of Authorized QoS: The PCRF may provide authorized QoS to the PCEF. The authorized QoS provides appropriate values for resources to be enforced.
- Policy Provisioning for Authorized QoS Per SDF: The provisioning of authorized QoS per SDF is a part of PCC rule provisioning procedure.
- Policy Enforcement for Authorized QoS Per SDF: If an authorized QoS is defined for a PCC rule, the PCEF limits the data rate of the SDF corresponding to that PCC rule not to exceed the maximum authorized bandwidth for the PCC rule by discarding packets exceeding the limit.
- Upon deactivation or removal of a PCC rule, the PCEF frees the resources reserved for that PCC rule.

Other Features

This section describes some of the other features.

PCC Rule Error Handling

If the installation/activation of one or more PCC rules fails, the PCEF communicates the failure to the PCRF by including one or more Charging-Rule-Report AVP(s) in either a CCR or an RAA command for the affected PCC rules. Within each Charging-Rule-Report AVP, the PCEF identifies the failed PCC rule(s) by including the Charging-Rule-Name AVP(s) or Charging-Rule-Base-Name AVP(s), identifies the failed reason code by including a Rule-Failure-Code AVP, and includes the PCC-Rule-Status AVP.

If the installation/activation of one or more new PCC rules (that is, rules that were not previously successfully installed) fail, the PCEF sets the PCC-Rule-Status to INACTIVE for both the PUSH and the PULL modes.

If a PCC rule was successfully installed/activated, but can no longer be enforced by the PCEF, the PCEF sends the PCRF a new CCR command and includes the Charging-Rule-Report AVP. The PCEF includes the Rule-Failure-Code AVP within the Charging-Rule-Report AVP and sets the PCC-Rule-Status to INACTIVE.

In the HA/PDSN Gx implementation, the following rule failure codes are supported:

- RATING_GROUP_ERROR (2)
- SERVICE_IDENTIFIER_ERROR (3)
- GW/PCEF_MALFUNCTION (4)
- RESOURCES_LIMITATION (5)

If the installation/activation of one or more PCC rules fails during RAR procedure, the RAA command is sent with the Experimental-Result-Code AVP set to DIAMETER_PCC_RULE_EVENT (5142).

Time of the Day Procedures

PCEF performs PCC rule request as instructed by the PCRF. Revalidation-Time when set by the PCRF, causes the PCEF to trigger a PCRF interaction to request PCC rules from the PCRF for an established IP-CAN session. The PCEF stops the timer once the PCEF triggers a REVALIDATION_TIMEOUT event.

When installed, the PCC rule is inactive. If Rule-Activation-Time / Rule-Deactivation-Time is specified, then the PCEF sets the rule active / inactive after that time.

Charging Control

Important: In the HA/PDSN Rel. 8 Gx implementation, offline charging is not supported.

Charging Control is the process of associating packets belonging to an SDF to a charging key, and applying online charging as appropriate. FBC handles differentiated charging of the bearer usage based on real-time analysis of the SDFs. In order to allow for charging control, the information in the PCC rule identifies the SDF and specifies the parameters for charging control. The PCC rule information may depend on subscription data.

Online charging is supported via the Gy interface. In the case of online charging, it is possible to apply an online charging action upon PCEF events (for example, re-authorization upon QoS change).

It is possible to indicate to the PCEF that interactions with the charging systems are not required for a PCC rule, that is to perform neither accounting nor credit control for this SDF, then neither online nor offline charging is performed.

Supported Features:

- Provisioning of charging-related information for the IP-CAN Session
- Provisioning of charging addresses: Primary or secondary event charging function name (Online Charging Server (OCS) addresses)

  Important: In the HA/PDSN Rel. 8 Gx implementation, provisioning of primary or secondary charging collection function name (Offline Charging Server (OFCS) addresses) over Gx is not supported.

- Provisioning of Default Charging Method

Charging Correlation

In the HA/PDSN Rel. 8 Gx implementation, Charging Correlation is not supported. PCRF provides the flow identifier, which uniquely identifies an IP flow in an IMS session.

Policy and Charging Control (PCC) Rules

A PCC rule enables the detection of an SDF and provides parameters for policy control and/or charging control. The purpose of the PCC rule is to:

- Detect a packet belonging to an SDF in case of both uplink and downlink IP flows based on SDF filters in the PCC rule (packet rule matching).

  If no PCC rule matches the packet, the packet is dropped.
- Identify the service that the SDF contributes to.
- Provide applicable charging parameters for an SDF.
- Provide policy control for an SDF.

The PCEF selects a PCC rule for each packet received by evaluating received packets against SDF filters of PCC rules in the order of precedence of the PCC rules. When a packet matches an SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied.

There are two types of PCC rules:

- Dynamic PCC Rules: Rules dynamically provisioned by the PCRF to the PCEF via the Gx interface. These PCC rules may be either predefined or dynamically generated in the PCRF. Dynamic PCC rules can be activated, modified, and deactivated at any time.
- Predefined PCC Rule: Rules preconfigured in the PCEF by the operators. Predefined PCC rules can be activated or deactivated by the PCRF at any time. Predefined PCC rules within the PCEF may be grouped allowing the PCRF to dynamically activate a set of PCC rules over the Gx reference point.

Important: A third kind of rule, the static PCC rule can be preconfigured in the chassis by the operators. Static PCC rules are not explicitly known in the PCRF, and are not under control of the PCRF. Static PCC rules are bound to general purpose bearer with no Gx control.

A PCC rule consists of:

- Rule Name: The rule name is used to reference a PCC rule in the communication between the PCEF and PCRF.
- Service Identifier: The service identifier is used to identify the service or the service component the SDF relates to.
- Service Data Flow Filter(s): The service flow filter(s) is used to select the traffic for which the rule applies.
- Precedence: For different PCC rules with overlapping SDF filter, the precedence of the rule determines which of these rules is applicable. When a dynamic PCC rule and a predefined PCC rule have the same priority, the dynamic PCC rule takes precedence.
- Gate Status: The gate status indicates whether the SDF, detected by the SDF filter(s), may pass (gate is open) or will be discarded (gate is closed) in uplink and/or in downlink direction.

- QoS Parameters: The QoS information includes the QoS class identifier (authorized QoS class for the SDF), and authorized bitrates for uplink and downlink.
- Charging Key (rating group)
- Other charging parameters: The charging parameters define whether online charging interfaces are used, on what level the PCEF will report the usage related to the rule, etc.

Important: Configuring the Metering Method and Reporting Level for dynamic PCC rules is not supported.

PCC rules also include Application Function (AF) record information for enabling charging correlation between the application and bearer layer if the AF has provided this information via the Rx interface. For IMS, this includes the IMS Charging Identifier (ICID) and flow identifiers.

PCC Procedures over Gx Reference Point

Request for PCC Rules

The PCEF, via the Gx reference point, requests for PCC rules in the following instances:

- At IP-CAN session establishment
- At IP-CAN session modification

PCC rules can also be requested as a consequence of a failure in the PCC rule installation/activation or enforcement without requiring an event trigger.

Provisioning of PCC Rules

The PCRF indicates, via the Rel. 8 Gx reference point, the PCC rules to be applied at the PCEF. This may be using one of the following procedures:

- PULL (provisioning solicited by the PCEF): In response to a request for PCC rules being made by the PCEF, the PCRF provisions PCC rules in the CC-Answer.
- PUSH (unsolicited provisioning): The PCRF may decide to provision PCC rules without obtaining a request from the PCEF. For example, in response to information provided to the PCRF via the Rx reference point, or in response to an internal trigger within the PCRF. To provision PCC rules without a request from the PCEF, the PCRF includes these PCC rules in an RA-Request message. No CCR/CCA messages are triggered by this RA-Request.

For each request from the PCEF or upon unsolicited provisioning, the PCRF provisions zero or more PCC rules. The PCRF may perform an operation on a single PCC rule by one of the following means:

- To activate or deactivate a PCC rule that is predefined at the PCEF, the PCRF provisions a reference to this PCC rule within a Charging-Rule-Name AVP and indicates the required action by choosing either the Charging-Rule-Install AVP or the Charging-Rule-Remove AVP.
- To install or modify a PCRF-provisioned PCC rule, the PCRF provisions a corresponding Charging-Rule-Definition AVP within a Charging-Rule-Install AVP.
- To remove a PCC rule which has previously been provisioned by the PCRF, the PCRF provisions the name of this rule as value of a Charging-Rule-Name AVP within a Charging-Rule-Remove AVP.

Selecting a PCC Rule for Uplink IP Packets

If PCC is enabled, the PCEF selects the applicable PCC rule for each received uplink IP packet within an IP-CAN session by evaluating the packet against uplink SDF filters of PCRF-provided or predefined active PCC rules of this IP-CAN session in the order of the precedence of the PCC rules.

Important: When a PCRF-provided PCC rule and a predefined PCC rule have the same precedence, the uplink SDF filters of the PCRF-provided PCC rule is applied first.

When a packet matches an SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied. Uplink IP packets which do not match any PCC rule of the corresponding IP-CAN session are discarded.

Selecting a PCC Rule for Downlink IP Packets

If PCC is enabled, the PCEF selects a PCC rule for each received downlink IP packet within an IP-CAN session by evaluating the packet against downlink SDF filters of PCRF-provided or predefined active PCC rules of the IP-CAN session in the order of precedence of the PCC rules.

Important: When a PCRF-provided PCC rule and a predefined PCC rule have the same precedence, the downlink SDF filters of the PCRF-provided PCC rule are applied first.

When a packet matches an SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied. Downlink IP packets that do not match any PCC rule of the IP-CAN session are discarded.

The following procedures are also supported:

- Indication of IP-CAN Session Termination: When the IP-CAN session is being terminated the PCEF contacts the PCRF.
- Request of IP-CAN Session Termination: If the PCRF decides to terminate an IP-CAN session due to an internal trigger or trigger from the SPR, the PCRF informs the PCEF. The PCEF acknowledges to the PCRF and instantly removes/deactivates all the PCC rules that have been previously installed or activated on that IP-CAN session.

  The PCEF applies IP-CAN specific procedures to terminate the IP-CAN session. The HA/PDSN sends a MIP Revocation Request with the teardown indicator set to indicate that the termination of the entire IP-CAN session is requested. Furthermore, the PCEF applies the “Indication of IP-CAN Session Termination” procedure.
- Use of the Supported-Features AVP during session establishment to inform the destination host about the required and optional features that the origin host supports.

How it Works

This section describes how HA/PDSN Rel. 8 Gx Interface support works.

The following figure and table explain the IMS Authorization process between a system and IMS components that is initiated by the UE.

In this example, the Diameter Policy Control Application (DPCA) is the Gx interface to the PCRF. The interface between IMSA with PCRF is the Gx interface, and the interface between Session Manager (SessMgr) and Online Charging Service (OCS) is the Gy interface. Note that the IMSA service and DPCA are part of SessMgr on the system and separated in the figure for illustration purpose only.

Figure 13. HA/PDSN Rel. 8 Gx IMS Authorization Call Flow

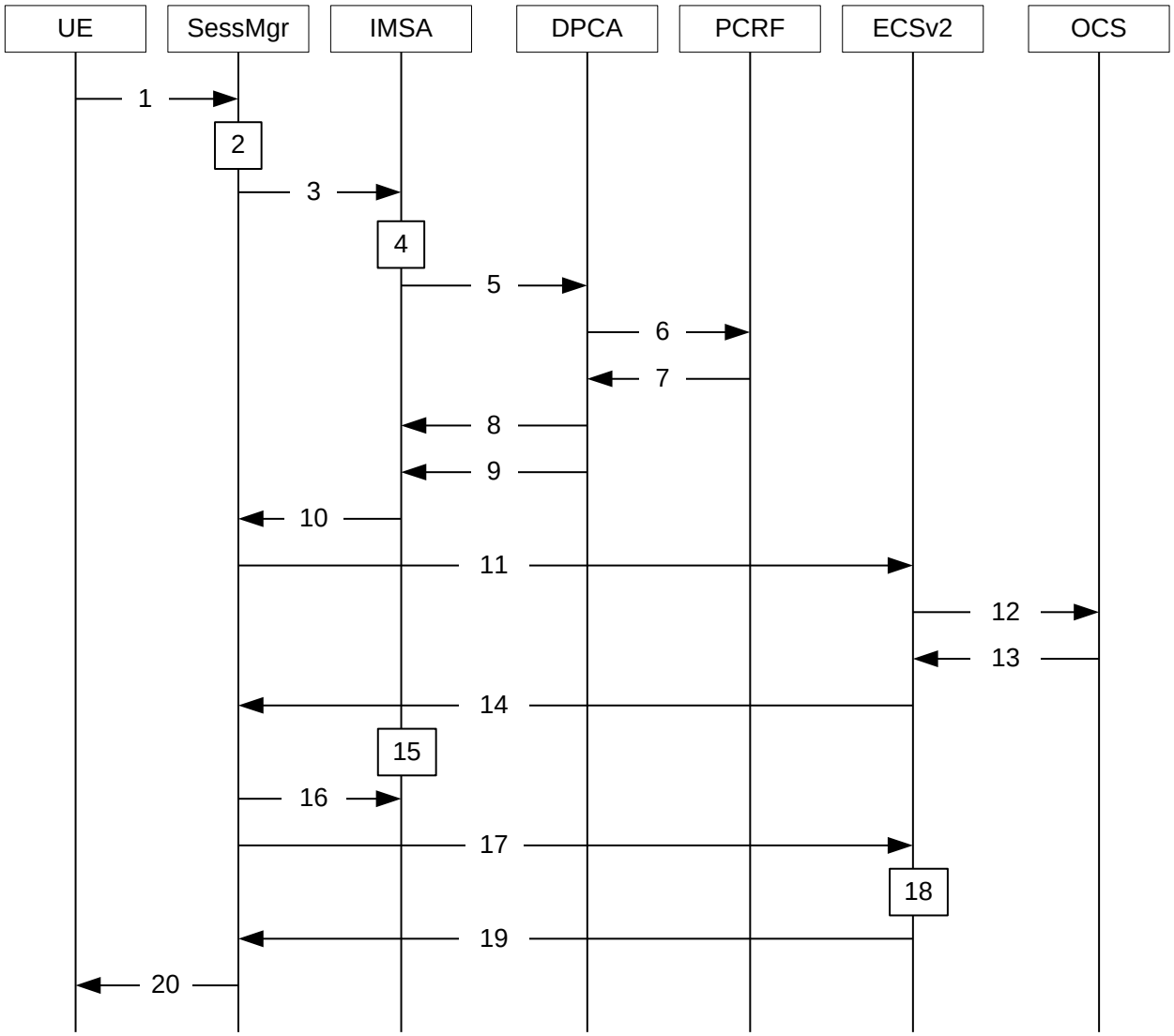


Table 5. HA/PDSN Rel. 8 Gx IMS Authorization Call flow Description

Step	Description
1	UE (IMS subscriber) requests for MIP Registration Request.
2	SessMgr allocates an IP address to the UE.
3	SessMgr requests IMS Authorization, if IMSA is enabled for the subscriber. IMSA service can either be configured in the subscriber template, or can be received from the AAA.
4	IMSA allocates resources for the IP-CAN session, and selects the PCRF to contact based on the user's selection key (for example, round-robin).
5	IMSA requests the DPCA module to issue an auth request to the PCRF.
6	DPCA sends a CCR initial message to the selected PCRF.
7	PCRF may send preconfigured charging rules in CCA. The dynamic rules and the authorized QoS parameters could also be included by the PCRF.
8	DPCA passes the charging rule definition, charging rule install, QoS information received from the PCRF, event triggers, etc. IMSA stores the information.
9	DPCA calls the callback function registered with it by IMSA.
10	PCRF-provided information common to the entire IP-CAN session (event trigger, primary/secondary OCS address, etc.) is stored within the IMSA. After processing the information, IMSA notifies the SessMgr about the policy authorization complete.
11	If the validation of the rules fails in IMSA/DPCA, a failure is notified to PCRF containing the Charging-Rule-Report AVP. Else, IMSA initiates creation of ECS session. The primary/secondary OCS server address, etc. are sent to the ECS from the SessMgr.
12	ECS performs credit authorization by sending CCR(I) to OCS with CC-Request-Type set to INITIAL_REQUEST to open the credit control session. This request includes the active Rulebase-Id (default rulebase ID from the AAA).
13	OCS returns a CCA initial message that may activate a statically configured Rulebase and may include preemptive quotas.
14	ECS responds to SessMgr with the response message.
15	SessMgr requests IMSA for the dynamic rules.
16	IMSA sends the dynamic rules to SessMgr. Note that until the MIP session is established, all RAR messages from the PCRF are rejected.
17	SessMgr sends the dynamic rule information to the ECS. The gate flow status information and the QoS per flow (charging rule) information are also sent in the message.
18	ECS activates the predefined rules received, and installs the dynamic rules received. Also, the gate flow status and the QoS parameters are updated by ECS as per the dynamic charging rules. The Gx rulebase is treated as an ECS group-of-ruledefs. The response message contains the Charging Rule Report conveying the status of the rule provisioning at the ECS.
19	If the provisioning of rules fails partially, the context setup is accepted, and a new CCR-U is sent to the PCRF with the Charging-Rule-Report containing the PCC rule status for the failed rules. If the provisioning of rules fails completely, the context setup is rejected.
20	Depending on the response for the MIP Session Authorization, SessMgr sends the response to the UE and activates/rejects the call. If the Charging-Rule-Report contains partial failure for any of the rules, the PCRF is notified, and the call is activated. If the Charging-Rule-Report contains complete failure, the call is rejected.

Configuring HA/PDSN Rel. 8 Gx Interface Support

To configure HA/PDSN Rel. 8 Gx Interface functionality:

1. At the context level, configure IMSA service for IMS subscribers as described in the Configuring IMS Authorization Service at Context Level section.
2. Within the same context, configure the subscriber template to use the IMSA service as described in the Applying IMS Authorization Service to Subscriber Template section.
3. Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Important: Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Cisco ASR 5000 Series Command Line Interface Reference* for complete information regarding all commands.

Configuring IMS Authorization Service at Context Level

Use the following example to configure IMSA service at context level for IMS subscribers:

```
configure
   context <context_name>
      ims-auth-service <imsa_service_name>
         policy-control
            diameter origin endpoint <endpoint_name>
            diameter dictionary <dictionary>
            diameter request-timeout <timeout_duration>
            diameter host-select table { 1 | 2 } algorithm round-robin
            diameter host-select row-precedence <precedence_value> table { 1 | 2
} host <primary_host_name> [ realm <primary_realm_id> ] [ secondary host
<secondary_host_name> [ realm <secondary_realm_id> ] ] [ -noconfirm ]
            failure-handling cc-request-type { any-request | initial-request |
terminate-request | update-request } { diameter-result-code { any-error |
<result_code> [ to <end_result_code> ] } } { continue | retry-and-terminate |
terminate }
            exit
         exit
```

```
diameter endpoint <endpoint_name> [ -noconfirm ]
   origin realm <realm_name>
   use-proxy
   origin host <host_name> address <ip_address>
   no watchdog-timeout
   response-timeout <timeout_duration>
   connection timeout <timeout_duration>
   connection retry-timeout <timeout_duration>
   peer <primary_peer_name> [ realm <primary_realm_name> ] address
<ip_address> [ port <port_number> ]
   peer <secondary_peer_name> [ realm <secondary_realm_name> ] address
<ip_address> [ port <port_number> ]
   end
```

Notes:

- *<context_name>* must be the name of the context where you want to enable IMSA service.
- *<imsa_service_name>* must be the name of the IMSA service to be configured for Rel. 8 Gx interface authentication.
- A maximum of 16 authorization services can be configured globally in a system. There is also a system limit for the maximum number of total configured services.
- To enable Rel. 8 Gx interface support, pertinent Diameter dictionary must be configured. For information on the specific Diameter dictionary to use, please contact your local service representative.
- The Round Robin algorithm for PCRF selection is effective only over a large number of PCRF selections, and not at a granular level.
- To configure the PCRF host destinations configured in the PCEF, use the diameter host-select CLI commands.
- To configure the PCEF to use a pre-defined rule when the Gx fails, set the **failure-handling cc-request-type** CLI to **continue**. Policies available/in use will continue to be used and there will be no further interaction with the PCRF.

Verifying the IMSA Service Configuration

To verify the IMSA service configuration:

- Change to the context where you enabled IMSA service by entering the following command:

  context *<context_name>*

- Verify the IMSA service's configuration by entering the following command:

  show ims-authorization service name *<imsa_service_name>*

Applying IMS Authorization Service to Subscriber Template

After configuring IMSA service at the context-level, within the same context subscriber template must be configured to use the IMSA service for IMS subscribers.

Use the following example to apply IMSA service functionality to subscriber template within the context previously configured in the Configuring IMS Authorization Service at Context Level section.

```
configure
   context <context_name>
      subscriber default
         encrypted password <encrypted_password>
         ims-auth-service <imsa_service_name>
         ip access-group <access_group_name> in
         ip access-group <access_group_name> out
         ip context-name <context_name>
         mobile-ip home-agent <ip_address>
         active-charging rulebase <rulebase_name>
         end
```

Notes:

- *<context_name>* must be the name of the context in which the IMSA service was configured.
- *<imsa_service_name>* must be the name of the IMSA service configured for IMS authentication in the context.
- The ECS rulebase must be configured in the subscriber template.
- Provided interpretation of the Gx rulebase (Charging-Rule-Base-Name AVP) from PCRF is chosen to be ECS group-of-ruledefs, configure the following command in the Active Charging Service Configuration Mode:

  policy-control charging-rule-base-name active-charging-group-of- ruledefs

Verifying the Subscriber Configuration

Verify the IMSA service configuration for subscriber(s) by entering the following command in the Exec CLI configuration mode:

show subscribers ims-auth-service *<imsa_service_name>*

Notes:

<imsa_service_name> must be the name of the IMSA service configured for IMS authentication.

Gathering Statistics

This section explains how to gather Rel. 8 Gx statistics and configuration information.

In the following table, the first column lists what statistics to gather, and the second column lists the action to perform.

Table 6. Gathering HA/PDSN Rel. 8 Gx Statistics and Information

Statistics/Information	Action to perform
Information and statistics specific to policy control in IMS Authorization service.	**show ims-authorization policy-control statistics**
Information and statistics specific to the authorization servers used for IMS Authorization service.	**show ims-authorization servers ims-auth-service**
Information of all IMS Authorization service.	**show ims-authorization service all**
Statistics of IMS Authorization service.	**show ims-authorization service statistics**
Information, configuration, and statistics of sessions active in IMS Authorization service.	**show ims-authorization sessions all**
Complete information, configuration, and statistics of sessions active in IMS Authorization service.	**show ims-authorization sessions full**
Summarized information of sessions active in IMS Authorization service.	**show ims-authorization sessions summary**
Complete statistics for active charging service sessions.	**show active-charging sessions full**
Information for all rule definitions configured in the service.	**show active-charging ruledef all**
Information for all rulebases configured in the system.	**show active-charging rulebase all**
Information on all group of ruledefs configured in the system.	**show active-charging group-of-ruledefs all**
Information on policy gate counters and status.	**show ims-authorization policy-gate { counters | status }**

P-GW Rel. 8 Gx Interface Support

Introduction

The Gx reference point is located between the Policy and Charging Rules Function (PCRF) and the Policy and Charging Enforcement Function (PCEF) on the Packet Data Network (PDN) Gateway (P-GW). The Gx reference point is used for provisioning and removal of PCC rules from the PCRF to the PCEF and the transmission of traffic plane events from the PCEF to the PCRF. The Gx reference point can be used for charging control, policy control, or both, by applying AVPs relevant to the application.

The PCEF is the functional element that encompasses policy enforcement and flow based charging functionality. This functional entity is located at the P-GW. The main functions include:

- Control over the user plane traffic handling at the gateway and its QoS.
- Service data flow detection and counting, as well as online and offline charging interactions.
- For a service data flow that is under policy control, the PCEF shall allow the service data flow to pass through the gateway if and only if the corresponding gate is open.
- For a service data flow that is under charging control, the PCEF shall allow the service data flow to pass through the gateway if and only if there is a corresponding active PCC rule and, for online charging, the OCS has authorized the applicable credit with that charging key.
- If requested by the PCRF, the PCEF shall report to the PCRF when the status of the related service data flow changes.
- In case the SDF is tunnelled at the BBERF, the PCEF shall inform the PCRF about the mobility protocol tunnelling header of the service data flows at IP-CAN session establishment.

Appendix C
Gy Interface Support

This chapter provides an overview of the Gy interface and describes how to configure the Gy interface.

Gy interface support is available on the Cisco ASR 5000 platform running StarOS 9.0 or later releases for the following products:

- GGSN
- HA
- IPSG
- PDSN
- P-GW

It is recommended that before using the procedures in this chapter you select the configuration example that best meets your service model, and configure the required elements for that model as described in this Administration Guide.

This chapter describes the following topics:

Introduction

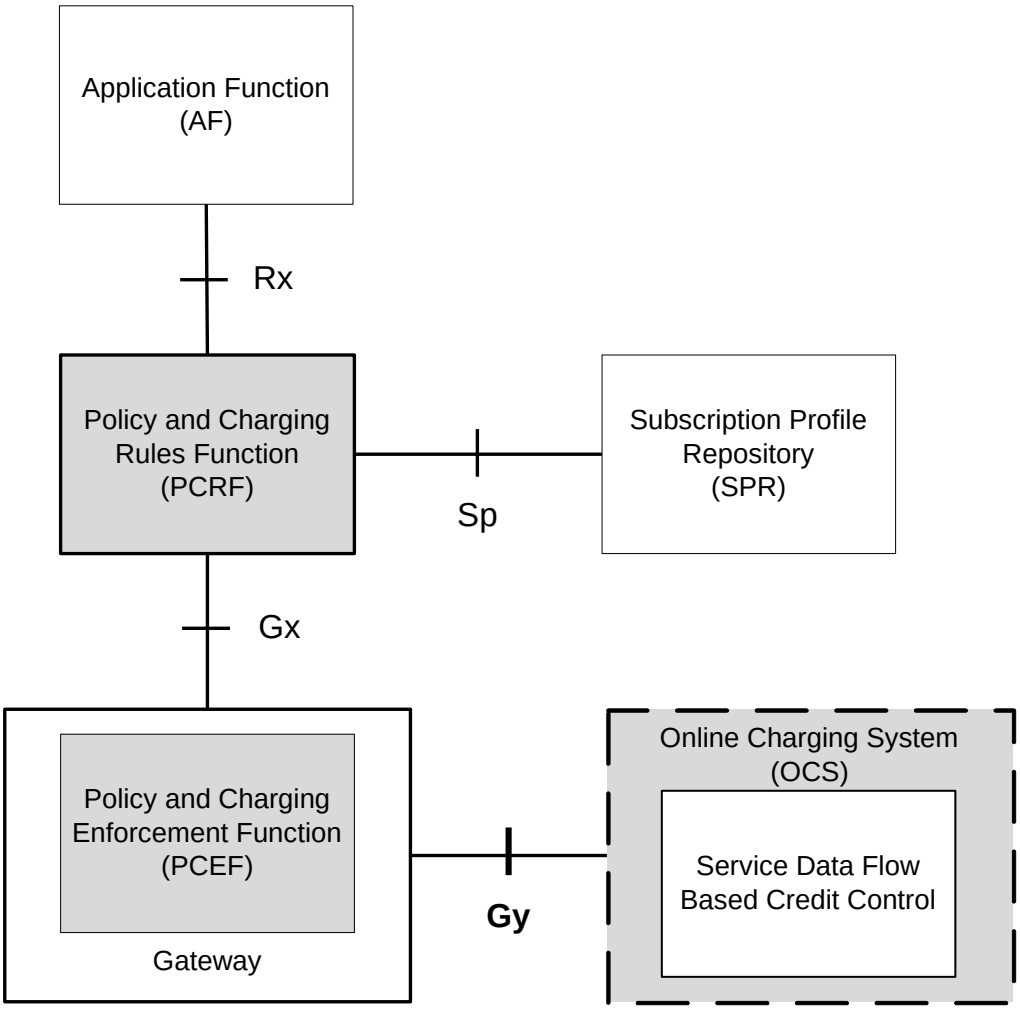
The Gy interface is the online charging interface between the PCEF/GW (Charging Trigger Function (CTF)) and the Online Charging System (Charging-Data-Function (CDF)).

The Gy interface makes use of the Active Charging Service (ACS) / Enhanced Charging Service (ECS) for real-time content-based charging of data services. It is based on the 3GPP standards and relies on quota allocation. The Online Charging System (OCS) is the Diameter Credit Control server, which provides the online charging data to the PCEF/GW. With Gy, customer traffic can be gated and billed in an online or prepaid style. Both time- and volume-based charging models are supported. In these models differentiated rates can be applied to different services based on ECS shallow- or deep-packet inspection.

In the simplest possible installation, the system will exchange Gy Diameter messages over Diameter TCP links between itself and one prepay server. For a more robust installation, multiple servers would be used. These servers may optionally share or mirror a single quota database so as to support Gy session failover from one server to the other. For a more scalable installation, a layer of proxies or other Diameter agents can be introduced to provide features such as multi-path message routing or message and session redirection features.

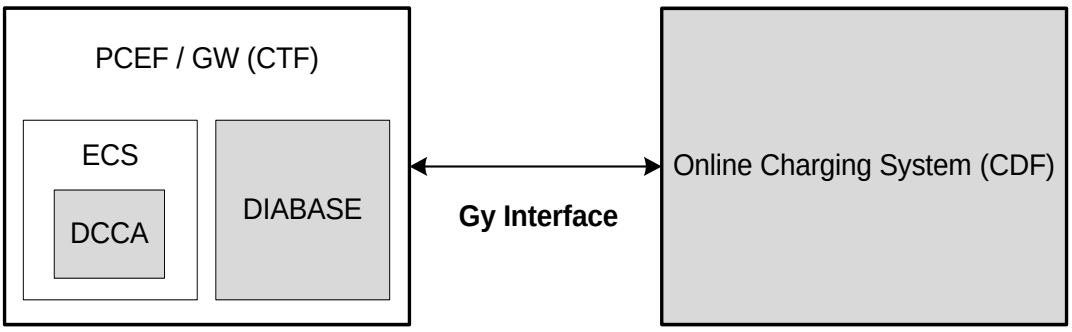
The following figure shows the Gy reference point in the policy and charging architecture.

Figure 14. PCC Logical Architecture



The following figure shows the Gy interface between CTF/Gateway/PCEF/Client running ECS and OCS (CDF/Server). Within the PCEF/GW, the Gy protocol functionality is handled in the DCCA module (at the ECS).

Figure 15. Gy Architecture



Licensing

Gy interface support requires the following license to be installed on the chassis:

Cisco PID [ASR5K-00-CS01ECG2] *Enhanced Charging Bundle 2, 1K Sessions*, or Starent Part Number [600-00-7574] *Enhanced Charging Bundle 2 1k Sessions* — To enable and configure Diameter and DCCA/Gy functionality with ECS.

For information on obtaining and installing licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *Cisco ASR 5000 Series System Administration Guide*.

Supported Standards

Gy interface support is based on the following standards:

- IETF RFC 4006: Diameter Credit Control Application; August 2005
- 3GPP TS 32.299 V9.6.0 (2010-12) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Diameter charging applications (Release 9)

Features and Terminology

This section describes features and terminology pertaining to Gy functionality.

Charging Scenarios

Important: Online charging for events (“Immediate Event Charging” and “Event Charging with Reservation”) is not supported. Only “Session Charging with Reservation” is supported.

Session Charging with Reservation

Session Charging with Unit Reservation is used for credit control of sessions.

Decentralized Unit Determination and Centralized Rating

In this scenario, the CTF requests the reservation of units prior to session supervision. An account debit operation is carried out following the conclusion of session termination.

Centralized Unit Determination and Centralized Rating

In this scenario, the CTF requests the OCS to reserve units based on the session identifiers specified by the CTF. An account debit operation is carried out following the conclusion of session.

Decentralized Unit Determination and Decentralized Rating

Important: Decentralized Rating is not supported in this release. Decentralized Unit determination is done using CLI configuration.

In this scenario, the CTF requests the OCS to assure the reservation of an amount of the specified number of monetary units from the subscriber's account. An account debit operation that triggers the deduction of the amount from the subscriber's account is carried out following the conclusion of session establishment.

Basic Operations

Important: Immediate Event Charging is not supported in this release. “Reserve Units Request” and “Reserve Units Response” are done for Session Charging and not for Event Charging.

Online credit control uses the basic logical operations “Debit Units” and “Reserve Units”.

- Debit Units Request; sent from CTF to OCS: After receiving a service request from the subscriber, the CTF sends a Debit Units Request to the OCS. The CTF may either specify a service identifier (centralised unit determination) or the number of units requested (decentralised unit determination). For refund purpose, the CTF sends a Debit Units Request to the OCS as well.
- Debit Units Response; sent from OCS to CTF: The OCS replies with a Debit Units Response, which informs the CTF of the number of units granted as a result of the Debit Units Request. This includes the case where the number of units granted indicates the permission to render the requested service. For refund purpose, the OCS replies with a Debit Units Response.
- Reserve Units Request; sent from CTF to OCS: Request to reserve a number of units for the service to be provided by an CTF. In case of centralised unit determination, the CTF specifies a service identifier in the Reserve Unit Request, and the OCS determines the number of units requested. In case of decentralised unit determination, the number of units requested is specified by the CTF.
- Reserve Units Response; sent from OCS to CTF: Response from the OCS which informs the CTF of the number of units that were reserved as a result of the “Reserve Units Request”.

Session Charging with Unit Reservation (SCUR) use both the “Debit Units” and “Reserve Units” operations. SCUR uses the Session Based Credit Control procedure specified in RFC 4006. In session charging with unit reservation, when the “Debit Units” and “Reserve Units” operations are both needed, they are combined in one message.

Important: Cost-Information, Remaining-Balance, and Low-Balance-Indication AVPs are not supported.

The consumed units are deducted from the subscriber's account after service delivery. Thus, the reserved and consumed units are not necessarily the same. Using this operation, it is also possible for the CTF to modify the current reservation, including the return of previously reserved units.

Re-authorization

The server may specify an idle timeout associated with a granted quota. Alternatively, the client may have a configurable default value. The expiry of that timer triggers a re-authorization request.

Mid-session service events (re-authorisation triggers) may affect the rating of the current service usage. The server may instruct the credit control client to re-authorize the quota upon a number of different session related triggers that can affect the rating conditions.

When a re-authorization is trigger, the client reports quota usage. The reason for the quota being reported is notified to the server.

Threshold based Re-authorization Triggers

The server may optionally include an indication to the client of the remaining quota threshold that triggers a quota re-authorization.

Termination Action

The server may specify to the client the behavior on consumption of the final granted units; this is known as termination action.

Diameter Base Protocol

The Diameter Base Protocol maintains the underlying connection between the Diameter Client and the Diameter Server. The connection between the client and server is TCP based. There are a series of message exchanges to check the status of the connection and the capabilities.

- Capabilities Exchange Messages: Capabilities Exchange Messages are exchanged between the diameter peers to know the capabilities of each other and identity of each other.
  - Capabilities Exchange Request (CER): This message is sent from the client to the server to know the capabilities of the server.
  - Capabilities Exchange Answer (CEA): This message is sent from the server to the client in response to the CER message.

    Important: Acct-Application-Id is not parsed and if sent will be ignored by the PCEF/GW. In case the Result-Code is not DIAMETER_SUCCESS, the connection to the peer is closed.

- Device Watchdog Request (DWR): After the CER/CEA messages are exchanged, if there is no more traffic between peers for a while, to monitor the health of the connection, DWR message is sent from the client. The Device Watchdog timer (Tw) is configurable in PCEF/GW and can vary from 6 through 30 seconds. A very low value will result in duplication of messages. The default value is 30 seconds. On two consecutive expiries of Tw without a DWA, the peer is taken to be down.

  Important: DWR is sent only after Tw expiry after the last message that came from the server. Say if there is continuous exchange of messages between the peers, DWR might not be sent if (Current Time - Last message received time from server) is less than Tw.

- Device Watchdog Answer (DWA): This is the response to the DWR message from the server. This is used to monitor the connection state.
- Disconnect Peer Request (DPR): This message is sent to the peer to inform to shutdown the connection. PCEF/GW only receives this message. There is no capability currently to send the message to the diameter server.

- Disconnect Peer Answer (DPA): This message is the response to the DPR request from the peer. On receiving the DPR, the peer sends DPA and puts the connection state to "DO NOT WANT TO TALK TO YOU" state and there is no way to get the connection back except for reconfiguring the peer again.

  A timeout value for retrying the disconnected peer must be provided.

- Tw Timer Expiry Behavior: The connection between the client and the server is taken care by the DIABASE application. When two consecutive Tw timers are expired, the peer state is set to idle and the connection is retried to be established. All the active sessions on the connection are then transferred to the secondary connection if one is configured. All new session activations are also tried on the secondary connection.

  There is a connection timeout interval, which is also equivalent to Tw timer, wherein after a CER has been sent to the server, if there is no response received while trying to reestablish connection, the connection is closed and the state set to idle.

Diameter Credit Control Application

The Diameter Credit Control Application (DCCA) is a part of the ECS subsystem. For every prepaid customer with Diameter Credit Control enabled, whenever a session comes up, the Diameter server is contacted and quota for the subscriber is fetched.

Quota Behavior

Various forms of quotas are present that can be used to charge the subscriber in an efficient way. Various quota mechanisms provide the end user with a variety of options to choose from and better handling of quotas for the service provider.

Time Quotas

The Credit-Control server can send the CC-Time quota for the subscriber during any of the interrogation of client with it. There are also various mechanisms as discussed below which can be used in conjunction with time quota to derive variety of methods for customer satisfaction.

- Quota Consumption Time: The server can optionally indicate to the client that the quota consumption must be stopped after a period equal to the "Quota Consumption Time" in which no packets are received or at session termination, whichever is sooner. The idle period equal to the Quota Consumption Time is included in the reported usage. The quota is consumed normally during gaps in traffic of duration less than or equal to the Quota-Consumption-Time. Quota consumption resumes on receipt of a further packet belonging to the service data flow.

  If packets are allowed to flow during a CCR (Update)/CCA exchange, and the Quota-Consumption-Time AVP value in the provided quota is the same as in the previously provided quota, then the Quota-Consumption-Time runs normally through this procedure. For example, if 5 seconds of a 10 second QCT timer have passed when a CCR(U) is triggered, and the CCA(U) returns 2 seconds later, then the QCT timer will expire 3 seconds after the receipt of the CCA and the remaining unaccounted 5 seconds of usage will be recorded against the new quota even though no packets were transmitted with the new quota.

  A locally configurable default value in the client can be used if the server doesn't send the QCT in the CCA.

- Combinational Quota: Discrete-Time-Period (DTP) and Continuous-Time-Period (CTP) defines mechanisms that extends and generalize the Quota-Consumption-Time for consuming time-quota.
  - Both DTP and CTP uses a “base-time-interval” that is used to create time-envelopes of quota used.
  - Instead of consuming the quota linearly, DTP and CTP consumes the granted quota discretely in chunks of base-time-interval at the start of the each base-time-interval.
  - Selection of one of this algorithm is based on the “Time-Quota-Mechanism” AVP sent by the server in CCA.
  - Reporting usage can also be controlled by Envelope-Reporting AVP sent by the server in CCA during the quota grant. Based on the value of this AVP, the usage can be reported either as the usage per envelope or as usual cumulative usage for that grant.
- Discrete-Time-Period: The base-time-interval defines the length of the Discrete-Time-Period. So each time-envelope corresponds to exactly one Discrete-Time-Period. So when a traffic is detected, an envelope of size equal to Base-Time-Interval is created. The traffic is allowed to pass through the time-envelope. Once the traffic exceeds the base-time-interval another new envelope equal to the base-time-interval is created. This continues till the quota used exceeds the quota grant or reaches the threshold limit for that quota.
- Continuous-Time-Period: Continuous time period mechanism constructs time envelope out of consecutive base-time intervals in which the traffic occurred up to and including a base time interval which contains no traffic. Therefore the quota consumption continues within the time envelope, if there was traffic in the previous base time interval. After an envelope has closed, then the quota consumption resumes only on the first traffic following the closure of the envelope. The envelope for CTP includes the last base time interval which contains no traffic.

  The size of the envelope is not constant as it was in Parking meter. The end of the envelope can only be determined retrospectively.
- Quota Hold Time: The server can specify an idle timeout associated with a granted quota using the Quota-Holding-Time AVP. If no traffic associated with the quota is observed for this time, the client understands that the traffic has stopped and the quota is returned to the server. The client starts the quota holding timer when quota consumption ceases. This is always when traffic ceases, i.e. the timer is re-started at the end of each packet. It applies equally to the granted time quota and to the granted volume quota. The timer is stopped on sending a CCR and re-initialized on receiving a CCA with the previous used value or a new value of Quota-Holding-Time if received.

  Alternatively, if this AVP is not present, a locally configurable default value in the client is used. A Quota-Holding-Time value of zero indicates that this mechanism is not used.
- Quota Validity Time: The server can optionally send the validity time for the quota during the interrogation with the client. The Validity-Time AVP is present at the MSCC level and applies equally to the entire quota that is present in that category. The quota gets invalidated at the end of the validity time and a CCR-Update is sent to the server with the Used-Service-Units AVP and the reporting reason as VALIDITY_TIME. The entire quota present in that category will be invalidated upon Quota-Validity-Time expiry and traffic in that category will be passed or dropped depending on the configuration, till a CCA-Update is received with quota for that category.

  Validity-Time of zero is invalid. Validity-Time is relative and not absolute.

Volume Quota

The server sends the CC-Total-Octets AVP to provide volume quota to the subscriber. DCCA currently supports only CC-Total-Octets AVP, which applies equally to uplink and downlink packets. If the total of uplink and downlink packets exceeds the CC-Total-Octets granted, the quota is assumed to be exhausted.

If CC-Input-Octets and/or CC-Output-Octets is provided, the quota is counted against CC-Input-Octets and/or CC-Output-Octets respectively.


Important: Restricting usages based on CC-Input-Octets and CC_Output-Octets is not supported in this release.

Units Quota

The server can also send a CC-Service-Specific-Units quota which is used to have packets counted as units. The number of units per packet is a configurable option.

Granting Quota

Gy implementation assumes that whenever the CC-Total-Octets AVP is present, volume quota has been granted for both uplink and downlink.

If the Granted-Service-Unit contains no data, Gy treats it as an invalid CCA.

If the values are zero, it is assumed that no quota was granted.

If the AVP contains the sub AVPs without any data, it is assumed to be infinite quota.

Additional parameters relating to a category like QHT, QCT is set for the category after receiving a valid volume or time grant.

If a default quota is configured for the subscriber, and subscriber traffic is received it is counted against the default quota. The default quota is applicable only to the initial request and is not regranted during the course of the session. If subscriber disconnects and reconnects, the default quota will be applied again for the initial request.

Requesting Quota

Quotas for a particular category type can be requested using the Requested-Service-Unit AVP in the CCR. The MSCC is filled with the Rating-Group AVP which corresponds to the category of the traffic and Requested-Service-Unit AVP without any data.

The Requested-Service-Unit can contain the CC AVPs used for requesting specific quantity of time or volume grant. Gy CLI can be used to request quota for a category type.

Alternatively quota can also be requested from the server preemptively for a particular category in CCR- I. When the server grants preemptive quota through the Credit control answer response, the quota will be used only when traffic is hit for that category. Quota can be preemptively requested from the Credit Control server from the CLI.

Reporting Quota

Quotas are reported to the server for number of reasons including:

- Threshold
- QHT Expiry
- Quota Exhaustion
- Rating Condition Change
- Forced Reauthorization
- Validity Time Expiry
- Final during Termination of Category Instance from Server

For the above cases except for QHT and Final, the Requested-Service-Unit AVP is present in the CCR.

Reporting Reason is present in CCR to let the server know the reason for the reporting of Quota. The Reporting-Reason AVP can be present either in MSCC level or at Used Service Unit (USU) level depending on whether the reason applies to all quotas or to single quota.

When one of these conditions is met, a CCR Update is sent to the server containing a Multiple-Services-Credit-Control AVP(s) indicating the reason for reporting usage in the Reporting-Reason and the appropriate value(s) for Trigger, where appropriate. Where a threshold was reached, the DCCA still has the amount of quota available to it defined by the threshold.

For all other reporting reasons the client discards any remaining quota and either discards future user traffic matching this category or allows user traffic to pass, or buffers traffic according to configuration.

For Reporting-Reason of Rating Condition Change, Gy requires the Trigger Type AVP to be present as part of the CCR to indicate which trigger event caused the reporting and re-authorization request.

For Reporting-Reason of end user service denied, this happens when a category is blacklisted by the credit control server, in this case a CCR-U is sent with used service unit even if the values as zero. When more quota is received from the server for that particular category, the blacklisting is removed.

If a default quota has been set for the subscriber then the usage from the default quota is deducted from the initial GSU received for the subscriber for the Rating Group or Rating Group and Service ID combination.

Default Quota Handling

- If default quota is set to 0, no data is passed/reported.
- If default quota is configured and default quota is not exhausted before OCS responds with quota, trafic is passed. Initial default quota used is counted against initial quota allocated. If quota allocated is less than the actual usage then actual usage is reported and additional quota requested. If no additional quota is available then traffic is denied.
- If default quota is not exhausted before OCS responds with denial of quota, gateway blocks traffic after OCS response. Gateway will report usage on default quota even in this case in CCR-U (FINAL) or CCR-T.
- if default quota is consumed before OCS responds, if OCS is not declared dead (see definition in use case 1 above) then traffic is blocked until OCS responds.

Thresholds

The Gy client supports the following threshold types:

- Volume-Quota-Threshold
- Time-Quota-Threshold
- Units-Quota-Threshold

A threshold is always associated with a particular quota and a particular quota type. in the Multiple-Services-Credit-Control AVP, the Time-Quota-Threshold, Volume-Quota-Threshold, and Unit-Quota-Threshold are optional AVPs.

They are expressed as unsigned numbers and the units are seconds for time quota, octets for volume quota and units for service specific quota. Once the quota has reached its threshold, a request for more quotas is triggered toward the server. User traffic is still allowed to flow. There is no disruption of traffic as the user still has valid quota.

The Gy sends a CCR Update with a Multiple-Services-Credit-Control AVP containing usage reported in one or more User-Service-Unit AVPs, the Reporting-Reason set to THRESHOLD and the Requested-Service-Unit AVP without data.

When quota of more than one type has been assigned to a category, each with its own threshold, then the threshold is considered to be reached once one of the unit types has reached its threshold even if the other unit type has not been consumed.

When reporting volume quota, the DCCA always reports uplink and downlink separately using the CC-Input-Octets AVP and the CC-Output-Octets AVP, respectively.

On receipt of more quotas in the CCA the Gy discard any quota not yet consumed since sending the CCR. Thus the amount of quota now available for consumption is the new amount received less any quota that may have been consumed since last sending the CCR.

Conditions for Reauthorization of Quota

Quota is re-authorized/requested from the server in case of the following scenarios:

- Threshold is hit
- Quota is exhausted
- Validity time expiry
- Rating condition change:
    - Cellid change: Applicable only to GGSN and P-GW implementations.
    - LAC change: Applicable only to GGSN and P-GW implementations.
    - QoS change
    - RAT change
    - SGSN/Serving-Node change: Applicable only to GGSN and P-GW implementations.

Discarding or Allowing or Buffering Traffic to Flow

Whenever Gy is waiting for CCA from the server, there is a possibility of traffic for that particular traffic type to be encountered in the Gy. The behavior of what needs to be done to the packet is determined by the configuration. Based on the configuration, the traffic is either allowed to pass or discarded or buffered while waiting for CCA from the server.

This behavior applies to all interrogation of client with server in the following cases:

- No quota present for that particular category
- Validity timer expiry for that category
- Quota exhausted for that category
- Forced Reauthorization from the server

In addition to allowing or discarding user traffic, there is an option available in case of quota exhausted or no quota circumstances to buffer the traffic. This typically happens when the server has been requested for more quota, but a valid quota response has not been received from the server, in this case the user traffic is buffered and on reception of valid quota response from the server the buffered traffic is allowed to pass through.

Procedures for Consumption of Time Quota

- QCT is zero: When QCT is deactivated, the consumption is on a wall-clock basis. The consumption is continuous even if there is no packet flow.
- QCT is active: When QCT is present in the CCA or locally configured for the session, then the consumption of quota is started only at the time of first packet arrival. The quota is consumed normally till last packet arrival plus QCT time and is passed till the next packet arrival.

  If the QCT value is changed during intermediate interrogations, then the new QCT comes into effect from the time the CCA is received. For instance, if the QCT is deactivated in the CCA, then quota consumptions resume normally even without any packet flow. Or if the QCT is activated from deactivation, then the quota consumption resume only after receiving the first packet after CCA.
- QHT is zero: When QHT is deactivated, the user holds the quota indefinitely in case there is no further usage (for volume quota and with QCT for time quota). QHT is active between the CCA and the next CCR.
- QHT is non-zero: When QHT is present in CCA or locally configured for the session, then after a idle time of QHT, the quota is returned to the server by sending a CCR-Update and reporting usage of the quota. On receipt of CCR-U, the server does not grant quota. QHT timer is stopped on sending the CCR and is restarted only if QHT is present in the CCA.

  QHT timer is reset every time a packet arrives.

Envelope Reporting

The server may determine the need for additional detailed reports identifying start time and end times of specific activity in addition to the standard quota management. The server controls this by sending a CCA with Envelope-Reporting AVP with the appropriate values. The DCCA client, on receiving the command, will monitor for traffic for a period of time controlled by the Quota-Consumption-Time AVP and report each period as a single envelope for each Quota-Consumption-Time expiry where there was traffic. The server may request envelope reports for just time or time and volume. Reporting the quota back to the server, is controlled by Envelope AVP with Envelope-Start-Time and Envelope-End-Time along with usage information.

Credit Control Request

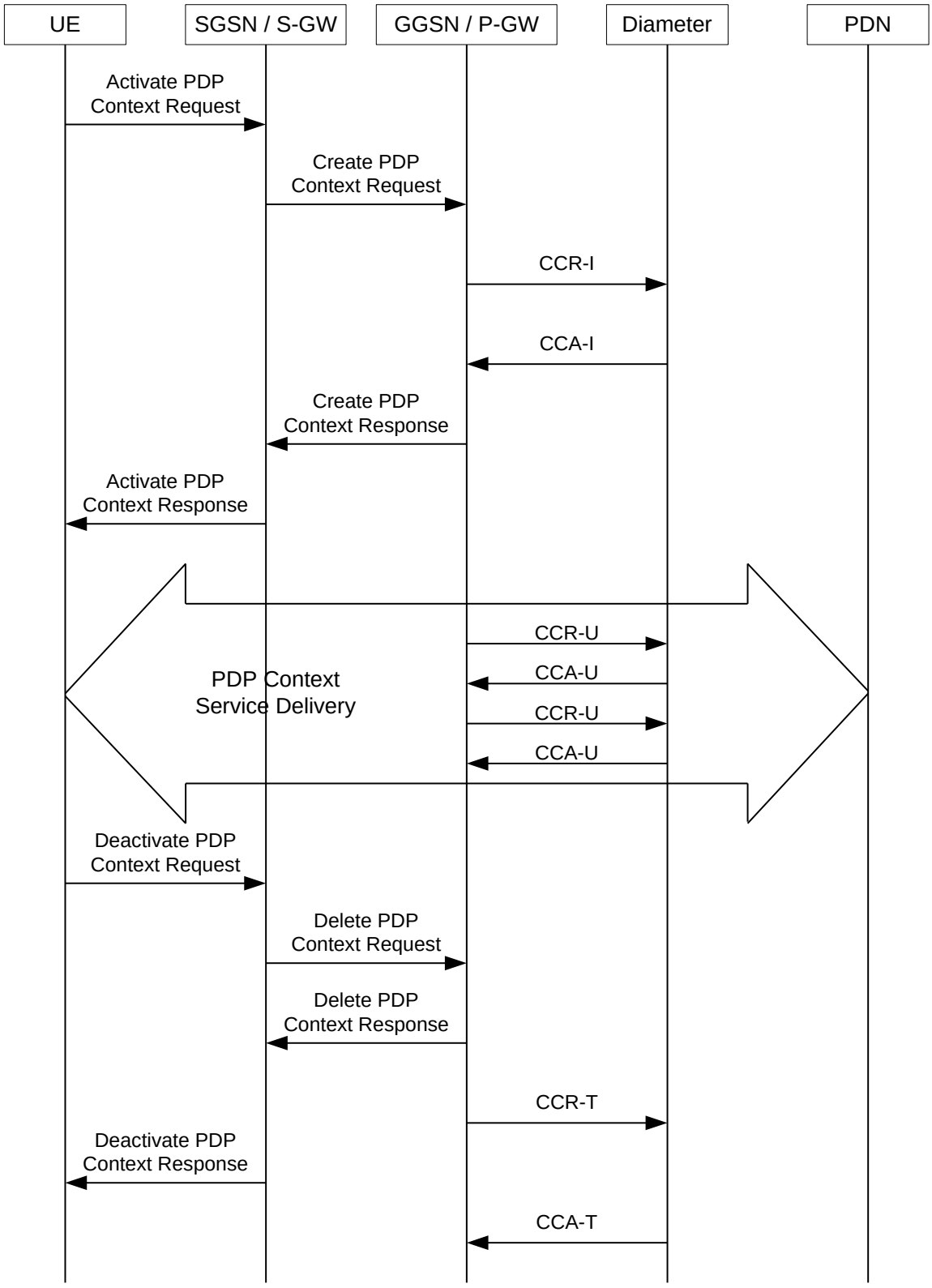
Credit Control Request (CCR) is the message that is sent from the client to the server to request quota and authorization. CCR is sent before the establishment of MIP session, and at the termination of the MIP session. It can be sent during service delivery to request more quotas.

- Credit Control Request - Initial (CCR-I)
- Credit Control Request - Update (CCR-U)
- Credit Control Request - Terminate (CCR-T)
- Credit Control Answer (CCA)
- Credit Control Answer - Initial (CCA-I)
- Credit Control Answer - Update (CCA-U)

  If the MSCC AVP is missing in CCA-Update it is treated as invalid CCA and the session is terminated.
- Credit Control Answer - Terminate (CCA-T)

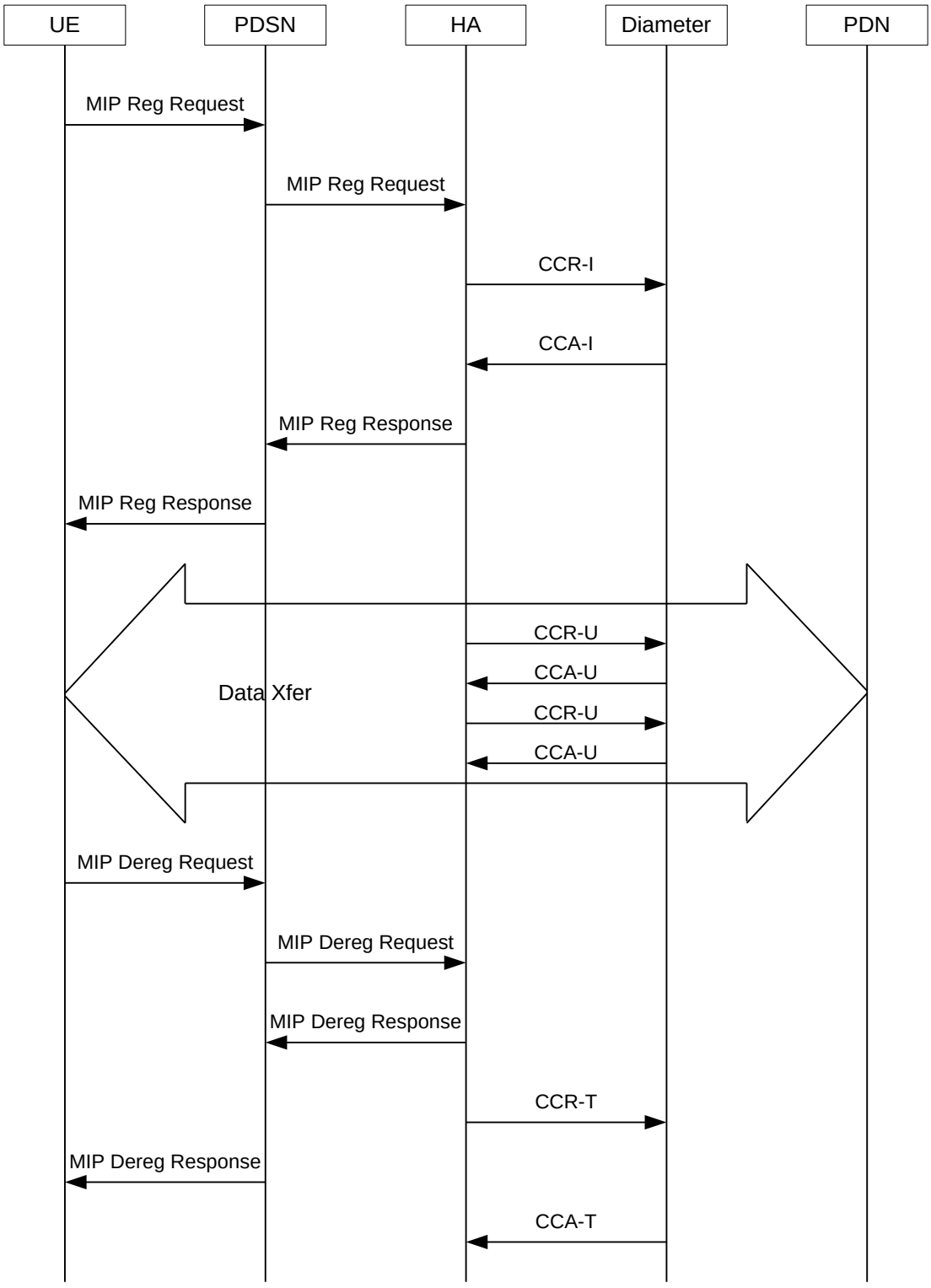
The following figure depicts the call flow for a simple call request in the GGSN / P-GW /IPSG Gy implementation.

Figure 16. Gy Call Flow for Simple Call Request



The following figure depicts the call flow for a simple call request in the HA Gy implementation.

Figure 17. Gy Call Flow for Simple Call Request



Tx Timer Expiry Behavior

A timer is started each time a CCR is sent out from the system, and the response has to arrive within Tx time. The timeout value is configurable in the Diameter Credit Control Configuration mode.

In case there is no response from the Diameter server for a particular CCR, within Tx time period, and if there is an alternate server configured, the CCR is sent to the alternate server after Tw expiry as described in "Tw Timer expiry behavior" section.

It also depends on the Credit-Control-Session-Failover AVP value for the earlier requests. If this AVP is present and is coded to FAILOVER_SUPPORTED then the credit-control message stream is moved to the secondary server, in case it is configured. If the AVP value is FAILOVER_NOT SUPPORTED, then the call is dropped in case of failures, even if a secondary server is configured.

Redirection

In the Final-Unit-Indication AVP, if the Final-Action is REDIRECT or Redirect-Server AVP is present at command level, redirection is performed.

The redirection takes place at the end of consumption of quota of the specified category. The GY sends a CCR-Update without any RSU or Rating-Group AVP so that the server does not give any more quotas.

If the Final-Action AVP is RESTRICT_ACCESS, then according to the settings in Restriction-Filter-Rule AVP or Filter-Id AVP. GY sends CCR-Update to the server with used quota.

Triggers

The Diameter server can provide with the triggers for which the client should reauthorize a particular category. The triggers can be configured locally as well but whatever trigger is present in the CCA from the server will have precedence.

Important: In this release, Gy triggers are not supported for HA.

The trigger types that are supported are:

- SGSN/Serving-Node Change
- QoS Change - Any
- RAT Change
- LAC Change
- CellID Change

On any event as described in the Trigger type happens, the client reauthorizes quota with the server. The reporting reason is set as RATING_CONDITION_CHANGE.

Tariff Time Change

The tariff change mechanism applies to each category instance active at the time of the tariff change whenever the server indicated it should apply for this category.

The concept of dual coupon is supported. Here the server grants two quotas, which is accompanied by a Tariff-Time-Change, in this case the first granted service unit is used until the tariff change time, once the tariff change time is reached the usage is reported up to the point and any additional usage is not accumulated, and then the second granted service unit is used.

If the server expects a tariff change to occur within the validity time of the quota it is granting, then it includes the Tariff-Time-Change AVP in the CCA. The DCCA report usage, which straddles the change time by sending two instances of the Used-Service-Unit AVP, one with Tariff-Change-Usage set to UNIT_BEFORE_TARIFF_CHANGE, and one with Tariff-Change-Usage set to UNIT_AFTER_TARIFF_CHANGE, and this independently of the type of units used by application. Both Volume and Time quota are reported in this way.

The Tariff time change functionality can as well be done using Validity-Time AVP, where in the Validity-Time is set to Tariff Time change and the client will reauthorize and get quota at Validity-Time expiry. This will trigger a lot of reauthorize request to the server at a particular time and hence is not advised.

Tariff-Time-Usage AVP along with the Tariff-Time-Change AVP in the answer message to the client indicates that the quotas defined in Multiple-Services-Credit-Control are to be used before or after the Tariff Time change. Two separate quotas are allocated one for before Tariff-Time-Change and one for after Tariff-Time-Change. This gives the flexibility to the operators to allocate different quotas to the users for different periods of time. In this case, the DCCA should not send the Before-Usage and After-Usage counts in the update messages to the server. When Tariff-Time-Change AVP is present without Tariff-Time-Usage AVP in the answer message, then the quota is used as in single quota mechanism and the client has to send before usage and after usage quotas in the updates to the server.

Important: In this release, Gy does not support UNIT_INDETERMINATE value.

Final Unit Indication

The Final-Unit-Indication AVP can be present in the CCA from the server to indicate that the given quota is the final quota from the server and the corresponding action as specified in the AVP needs to be taken.

Final Unit Indication at Command Level

Gy currently does not support FUI AVP at command level. If this AVP is present at command level it is ignored. If the FUI AVP is present at command level and the Final-Unit-Action AVP set to TERMINATE, Gy sends a CCR-Terminate at the expiry of the quota, with all quotas in the USU AVP.

Important: FUI AVP at command level is only supported for Terminate action.

Final Unit Indication at MSCC Level

If the Final-Unit-Indication AVP is present at MSCC level, and if the Final-Unit-Action AVP is set to TERMINATE, a CCR-Update is sent at the expiry of the allotted quota and report the usage of the category that is terminated.

For information on redirection cases refer to the Redirection section.

Credit Control Failure Handling

CCFH AVP defines what needs to be done in case of failure of any type between the client and the server. The CCFH functionality can be defined in configuration but if the CCFH AVP is present in the CCA, it takes precedence. CCFH AVP gives flexibility to have different failure handling.

Gy supports the following Failure Handling options:

- TERMINATE
- CONTINUE
- RETRY AND TERMINATE

CCFH with Failover Supported

In case there is a secondary server is configured and if the CC-Session-Failover AVP is set to FAILOVER_SUPPORTED, the following behavior takes place:

- Terminate: On any Tx expiry for the CCR-I the message is discarded and the session is torn down. In case of CCR-Updates and Terminates the message is sent to the secondary server after response timeout and the session is proceeded with the secondary server. In case there is a failure with the secondary server too, the session is torn down.
- Continue: On any Tx expiry, the message is sent to the secondary server after response timeout and the session is proceeded with the secondary server. In case there is a failure with the secondary server too, the session is still established, but without quota management.
- Retry and Terminate: On any Tx expiry, the message is sent to the secondary server after the response timeout. In case there is a failure with secondary server too, the session is taken down.

CCFH with Failover Not Supported

In case there is a secondary server configured and if the CC-Session-Failover AVP is set to FAILOVER_NOT_SUPPORTED, the following behavior takes place as listed below. Same is the case if there is no secondary server configured on the system.

- Terminate: On any Tx expiry, the session is taken down.
- Continue: On any Tx expiry, the session is still established, but without quota management.
- Retry and Terminate: On any Tx expiry, the session is taken down.

Failover Support

The CC-Session-Failover AVP and the Credit-Control-Failure-Handling (CCFH) AVP may be returned by the CC server in the CCA-I, and are used by the DCCA to manage the failover procedure. If they are present in the CCA they override the default values that are locally configured in the system.

If the CC-Session-Failover is set to FAILOVER_NOT_SUPPORTED, a CC session will never be moved to an alternative Diameter Server.

If the value of CC-Session-Failover is set to FAILOVER_SUPPORTED, then the Gy attempts to move the CC session to the alternative server when it considers a request to have failed, i.e:

- On receipt of result code “DIAMETER_UNABLE_TO_DELIVER”, “DIAMETER_TOO_BUSY”, or “DIAMETER_LOOP_DETECTED”.
- On expiry of the request timeout.
- On expiry of Tw without receipt of DWA, if the server is connected directly to the client.

The CCFH determines the behavior of the client in fault situations. If the Tx timer expires then based on the CCFH value the following actions are taken:

- CONTINUE: Allow the MIP session and user traffic for the relevant category or categories to continue, regardless of the interruption (delayed answer). Note that quota management of other categories is not affected.
- TERMINATE: Terminate the MIP session, which affects all categories.
- RETRY_AND_TERMINATE: Allow the MIP session and user traffic for the relevant category or categories to continue, regardless of the interruption (delayed answer). The client retries to send the CCR when it determines a failure-to-send condition and if this also fails, the MIP session is then terminated.

After the failover action has been attempted, and if there is still a failure to send or temporary error, depending on the CCFH action, the following action is taken:

- CONTINUE: Allow the MIP session to continue.
- TERMINATE: Terminate the MIP session.
- RETRY_AND_TERMINATE: Terminate the MIP session.

Recovery Mechanisms

DCCA supports a recovery mechanism that is used to recover sessions without much loss of data in case of Session Manager failures. There is a constant check pointing of Gy data at regular intervals and at important events like update, etc.

For more information on recovery mechanisms, please refer to the *Cisco ASR 5000 Series System Administration Guide*.

Error Mechanisms

Unsupported AVPs

All unsupported AVPs from the server with "M" bit set are ignored.

Invalid Answer from Server

If there is an invalid answer from the server, Gy action is dependent on the CCFH setting:

- In case of continue, the MIP session context is continued without further control from Gy.
- In case of terminate and retry-and-terminate, the MIP session is terminated and a CCR-T is sent to the diameter server.

Result Code Behavior

- DIAMETER_RATING_FAILED: On reception of this code, Gy discards all traffic for that category and does not request any more quota from the server. This is supported at the MSCC level and not at the command level.
- DIAMETER_END_USER_SERVICE_DENIED: On reception of this code, Gy temporarily blacklists the category and further traffic results in requesting new quota from the server. This is supported at the MSCC level and not at the command level.
- DIAMETER_CREDIT_LIMIT_REACHED: On reception of this code, Gy discards all traffic for that category and waits for a configured time, after which if there is traffic for the same category requests quota from the server. This is supported at the MSCC level and not at the command level.
- DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE: On reception of this code, Gy allows the session to establish, but without quota management. This is supported only at the command level and not at the MSCC level.
- DIAMETER_USER_UNKNOWN: On reception of this code, DCCA does not allow the credit control session to get established, the session is terminated. This result code is supported only at the command level and not at the MSCC level.

For all other permanent/transient failures, Gy action is dependent on the CCFH setting.

Supported AVPs

The Gy functionality supports the following AVPs:

- Supported Diameter Credit Control AVPs specified in RFC 4006:
  - CC-Input-Octets (AVP Code: 412):

    Gy supports this AVP only in USU.
  - CC-Output-Octets (AVP Code: 414):

    Gy supports this AVP only in USU.
  - CC-Request-Number (AVP Code: 415)

- CC-Request-Type (AVP Code: 416):

  Gy currently does not support EVENT_REQUEST value.
- CC-Service-Specific-Units (AVP Code: 417)
- CC-Session-Failover (AVP Code: 418)
- CC-Time (AVP Code: 420):

  Gy does not support this AVP in RSU.
- CC-Total-Octets (AVP Code: 421):

  Gy does not support this AVP in RSU.
- Credit-Control-Failure-Handling (AVP Code: 427)
- Final-Unit-Action (AVP Code: 449):

  Supported at Multiple-Services-Credit-Control grouped AVP level and not at command level.
- Final-Unit-Indication (AVP Code: 430):

  Fully supported at Multiple-Services-Credit-Control grouped AVP level and partially supported (TERMINATE) at command level.
- Granted-Service-Unit (AVP Code: 431)
- Multiple-Services-Credit-Control (AVP Code: 456)
- Multiple-Services-Indicator (AVP Code: 455)
- Rating-Group (AVP Code: 432)
- Redirect-Address-Type (AVP Code: 433):

  Gy currently supports only URL (2) value.
- Redirect-Server (AVP Code: 434)
- Redirect-Server-Address (AVP Code: 435)
- Requested-Service-Unit (AVP Code: 437)
- Result-Code (AVP Code: 268)
- Service-Context-Id (AVP Code: 461)
- Service-Identifier (AVP Code: 439)
- Subscription-Id (AVP Code: 443)
- Subscription-Id-Data (AVP Code: 444)
- Subscription-Id-Type (AVP Code: 450)
- Tariff-Change-Usage (AVP Code: 452):

  Gy does NOT support UNIT_INDETERMINATE (2) value.
- Tariff-Time-Change (AVP Code: 451)
- Used-Service-Unit (AVP Code: 446):

  Gy sends only incremental counts for all the AVPs from the last CCA-U.
- User-Equipment-Info (AVP Code: 458)
- User-Equipment-Info-Type (AVP Code: 459):

  Gy currently supports only IMEISV value.

Cisco GGSN and P-GW support IMEISV by default.

- User-Equipment-Info-Value (AVP Code: 460)
- Validity-Time (AVP Code: 448)

- Supported 3GPP specific AVPs specified in 3GPP TS 32.299:
  - 3GPP-Charging-Characteristics (AVP Code: 13)
  - 3GPP-Charging-Id (AVP Code: 2)
  - 3GPP-GGSN-MCC-MNC (AVP Code: 9)
  - 3GPP-GPRS-QoS-Negotiated-Profile (AVP Code: 5)
  - 3GPP-IMSI-MCC-MNC (AVP Code: 8)
  - 3GPP-NSAPI (AVP Code: 10)
  - 3GPP-PDP-Type (AVP Code: 3)
  - 3GPP-RAT-Type (AVP Code: 21)
  - 3GPP-Selection-Mode (AVP Code: 12)
  - 3GPP-Session-Stop-Indicator (AVP Code: 11)
  - 3GPP-SGSN-MCC-MNC (AVP Code: 18)
  - 3GPP-User-Location-Info (AVP Code: 22)
  - Base-Time-Interval (AVP Code: 1265)
  - Charging-Rule-Base-Name (AVP Code: 1004)
  - Envelope (AVP Code: 1266)
  - Envelope-End-Time (AVP Code: 1267)
  - Envelope-Reporting (AVP Code: 1268)
  - Envelope-Start-Time (AVP Code: 1269)
  - GGSN-Address (AVP Code: 847)
  - Offline-Charging (AVP Code: 1278)
  - PDP-Address (AVP Code: 1227)
  - PDP-Context-Type (AVP Code: 1247)

    This AVP is present only in CCR-I.
  - PS-Information (AVP Code: 874)
  - Quota-Consumption-Time (AVP Code: 881):

    This optional AVP is present only in CCA.
  - Quota-Holding-Time (AVP Code: 871):

    This optional AVP is present only in the CCA command. It is contained in the Multiple-Services-Credit-Control AVP. It applies equally to the granted time quota and to the granted volume quota.
  - Reporting-Reason (AVP Code: 872):

    Gy currently does not support the POOL_EXHAUSTED (8) value. It is used in case of credit-pooling which is currently not supported.
  - Service-Information (AVP Code: 873):

Only PS-Information is supported.

- SGSN-Address (AVP Code: 1228)
- Time-Quota-Mechanism (AVP Code: 1270):

  The Gy server may include this AVP in an Multiple-Services-Credit-Control AVP when granting time quota.
- Time-Quota-Threshold (AVP Code: 868)
- Time-Quota-Type (AVP Code: 1271)
- Trigger (AVP Code: 1264)
- Trigger-Type (AVP Code: 870)
- Unit-Quota-Threshold (AVP Code: 1226)
- Volume-Quota-Threshold (AVP Code: 869)

- Supported Diameter AVPs specified in 3GPP TS 32.299 V8.1.0:
  - Auth-Application-Id (AVP Code: 258)
  - Destination-Host (AVP Code: 293)
  - Destination-Realm (AVP Code: 283)
  - Disconnect-Cause (AVP Code: 273)
  - Error-Message (AVP Code: 281)
  - Event-Timestamp (AVP Code: 55)
  - Failed-AVP (AVP Code: 279)
  - Multiple-Services-Credit-Control (AVP Code: 456)
  - Origin-Host (AVP Code: 264)
  - Origin-Realm (AVP Code: 296)
  - Origin-State-Id (AVP Code: 278)
  - Redirect-Host (AVP Code: 292)
  - Redirect-Host-Usage (AVP Code: 261)
  - Redirect-Max-Cache-Time (AVP Code: 262)
  - Rating-Group (AVP Code: 432)
  - Result-Code (AVP Code: 268)
  - Route-Record (AVP Code: 282)
  - Session-Id (AVP Code: 263)
  - Service-Context-Id (AVP Code: 461)
  - Service-Identifier (AVP Code: 439)
  - Supported-Vendor-Id (AVP Code: 265)
  - Termination-Cause (AVP Code: 295)
  - Used-Service-Unit (AVP Code: 446)
  - User-Name (AVP Code: 1)

Unsupported AVPs

This section lists the AVPs that are NOT supported.

- NOT Supported Credit Control AVPs specified in RFC 4006:
  - CC-Correlation-Id
  - CC-Money
  - CC-Sub-Session-Id
  - CC-Unit-Type (AVP Code: 454)
  - Check-Balance-Result
  - Cost-Information (AVP Code: 423)
  - Cost-Unit (AVP Code: 445)
  - Credit-Control
  - Currency-Code (AVP Code: 425)
  - Direct-Debiting-Failure-Handling (AVP Code: 428)
  - Exponent (AVP Code: 429)
  - G-S-U-Pool-Identifier (AVP Code: 453)
  - G-S-U-Pool-Reference (AVP Code: 457)
  - Requested-Action (AVP Code: 436)
  - Service-Parameter-Info (AVP Code: 440)
  - Service-Parameter-Type (AVP Code: 441)
  - Service-Parameter-Value (AVP Code: 442)
  - Unit-Value (AVP Code: 424)
  - Value-Digits (AVP Code: 447)
- NOT supported Diameter AVPs specified in 3GPP TS 32.299 V8.1.0:
  - Acct-Application-Id (AVP Code: 259)
  - Error-Reporting-Host (AVP Code: 294)
  - Experimental-Result (AVP Code: 297)
  - Experimental-Result-Code (AVP Code: 298)
  - Proxy-Host
  - Proxy-Info
  - Proxy-State
- NOT supported 3GPP-specific AVPs specified in 3GPP TS 32.299 V8.1.0:
  - 3GPP-CAMEL-Charging-Info (AVP Code: 24)
  - 3GPP-MS-TimeZone (AVP Code: 23)
  - 3GPP-PDSN-MCC-MNC
  - Authorised-QoS

- Access-Network-Information
- Adaptations
- Additional-Content-Information
- Additional-Type-Information
- Address-Data
- Address-Domain
- Addressee-Type
- Address-Type
- AF-Correlation-Information
- Alternate-Charged-Party-Address
- Application-provided-Called-Party-Address
- Application-Server
- Application-Server-Information
- Applic-ID
- Associated-URI
- Aux-Applic-Info
- Bearer-Service
- Called-Asserted-Identity
- Called-Party-Address
- Calling-Party-Address
- Cause-Code
- Charged-Party
- Class-Identifier
- Content-Class
- Content-Disposition
- Content-Length
- Content-Size
- Content-Type
- Data-Coding-Scheme
- Deferred-Location-Event-Type
- Delivery-Report-Requested
- Destination-Interface
- Domain-Name
- DRM-Content

- Early-Media-Description
- Event
- Event-Type
- Expires
- File-Repair-Supported
- IM-Information
- IMS-Charging-Identifier (ICID)
- IMS-Communication-Service-Identifier
- IMS-Information
- Incoming-Trunk-Group-ID
- Interface-Id
- Interface-Port
- Interface-Text
- Interface-Type
- Inter-Operator-Identifier
- LCS-APN
- LCS-Client-Dialed-By-MS
- LCS-Client-External-ID
- LCS-Client-ID
- LCS-Client-Name
- LCS-Client-Type
- LCS-Data-Coding-Scheme
- LCS-Format-Indicator
- LCS-Information
- LCS-Name-String
- LCS-Requestor-ID
- LCS-Requestor-ID-String
- Location-Estimate
- Location-Estimate-Type
- Location-Type
- Low-Balance-Indication
- MBMS-Information
- MBMS-User-Service-Type
- Media-Initiator-Flag

- Media-Initiator-Party
- Message-Body
- Message-Class
- Message-ID
- Message-Size
- Message-Type
- MMBox-Storage-Requested
- MM-Content-Type
- MMS-Information
- Node-Functionality
- Number-Of-Participants
- Number-Of-Received-Talk-Bursts
- Number-Of-Talk-Bursts
- Originating-IOI
- Originator
- Originator-Address
- Originator-Interface
- Originator-SCCP-Address
- Outgoing-Trunk-Group-ID
- Participant-Access-Priority
- Participants-Group
- Participants-Involved
- PDG-Address
- PDG-Charging-Id
- PoC-Change-Condition
- PoC-Change-Time
- PoC-Controlling-Address
- PoC-Group-Name
- PoC-Information
- PoC-Server-Role
- PoC-Session-Id
- PoC-Session-Initialtion-Type
- PoC-Session-Type
- PoC-User-Role

- PoC-User-Role-IDs
- PoC-User-Role-info-Units
- Positioning-Data
- Priority
- PS-Append-Free-Format-Data (AVP Code: 867):

  The PCEF/GW ignores this AVP if no PS free format data is stored for the online charging session.
- PS-Free-Format-Data (AVP Code: 866)
- PS-Furnish-Charging-Information (AVP Code: 865)
- RAI (AVP Code: 909)
- Read-Reply-Report-Requested
- Received-Talk-Burst-Time
- Received-Talk-Burst-Volume
- Recipient-Address
- Recipient-SCCP-Address
- Refund-Information
- Remaining-Balance
- Reply-Applic-ID
- Reply-Path-Requested
- Requested-Party-Address
- Role-of-node
- SDP-Answer-Timestamp
- SDP-Media-Component
- SDP-Media-Description
- SDP-Media-Name
- SDP-Offer-Timestamp
- SDP-Session-Description
- SDP-TimeStamp
- Served-Party-IP-Address
- Service-Generic-Information
- Service-ID
- Service-Specific-Data
- Service-Specific-Info
- Service-Specific-Type
- SIP-Method
- SIP-Request-Timestamp

- SIP-Response-Timestamp
- SM-Discharge-Time
- SM-Message-Type
- SM-Protocol-Id
- SMSC-Address
- SMS-Information
- SMS-Node
- SM-Status
- SM-User-Data-Header
- Submission-Time
- Talk-Burst-Exchange
- Talk-Burst-Time
- Talk-Burst-Volume
- Terminating-IOI
- Time-Stamps
- Token-Text
- Trunk-Group-ID
- Type-Number
- User-Participating-Type
- User-Session-ID
- WAG-Address
- WAG-PLMN-Id
- WLAN-Information
- WLAN-Radio-Container
- WLAN-Session-Id
- WLAN-Technology
- WLAN-UE-Local-IPAddress

Configuring Gy Interface Support

To configure Gy interface support:

1. Configure the core network service as described in this Administration Guide.
2. Configure Gy interface support as described in the relevant section:
   - Configuring GGSN / P-GW / IPSG Gy Interface Support
   - Configuring HA / PDSN Gy Interface Support
3. Verify and save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Important: Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Cisco ASR 5000 Series Command Line Interface Reference* for complete information regarding all commands.

Configuring GGSN / P-GW / IPSG Gy Interface Support

To configure the standard Gy interface support for GGSN/P-GW/IPSG, use the following configuration:

```
configure
   context <context_name>
      diameter endpoint <endpoint_name>
         origin realm <realm>
         origin host <diameter_host> address <ip_address>
         peer <peer> realm <realm> address <ip_address>
         exit
      exit
   active-charging service <ecs_service_name>
      credit-control [ group <cc_group_name> ]
         diameter origin endpoint <endpoint_name>
         diameter peer-select peer <peer> realm <realm>
         diameter pending-timeout <timeout_period>
         diameter session failover
```

```
      diameter dictionary <dictionary>
      failure-handling initial-request continue
      failure-handling update-request continue
      failure-handling terminate-request continue
      exit
   exit
context <context_name>
   apn <apn_name>
      selection-mode sent-by-ms
      ims-auth-service <service>
      ip access-group <access_list_name> in
      ip access-group <access_list_name> out
      ip context-name <context_name>
      active-charging rulebase <rulebase_name>
      credit-control-group <cc_group_name>
      end
```

Notes:

- For information on configuring IP access lists, refer to the *Access Control Lists* chapter in the *Cisco ASR 5000 Series System Administration Guide*.
- For more information on configuring ECS ruledefs, refer to the *ACS Ruledef Configuration Mode Commands* chapter in the *Cisco ASR 5000 Series Command Line Interface Reference*.
- For more information on configuring ECS charging actions, refer to the *ACS Charging Action Configuration Mode Commands* chapter in the *Cisco ASR 5000 Series Command Line Interface Reference*.
- For more information on configuring ECS rulebases, refer to the *ACS Rulebase Configuration Mode Commands* chapter in the *Cisco ASR 5000 Series Command Line Interface Reference*.

Configuring HA / PDSN Gy Interface Support

To configure HA / PDSN Gy interface support, use the following configuration:

```
configure
   context <context_name>
      diameter endpoint <endpoint_name>
         origin realm <realm>
         origin host <diameter_host> address <ip_address>
         peer <peer> realm <realm> address <ip_address>
         exit
      exit
   active-charging service <ecs_service_name>
      ruledef <ruledef_name>
         ip any-match = TRUE
         exit
      charging-action <charging_action_name>
         content-id <content_id>
         cca charging credit rating-group <rating_group>
         exit
      rulebase <rulebase_name>
         action priority <action_priority> ruledef <ruledef_name> charging-
action <charging_action_name>
         exit
      credit-control [ group <cc_group_name> ]
         diameter origin endpoint <endpoint_name>
         diameter peer-select peer <peer> realm <realm>
         diameter pending-timeout <timeout>
         diameter session failover
         diameter dictionary <dictionary>
```

```
        failure-handling initial-request continue
        failure-handling update-request continue
        failure-handling terminate-request continue
        pending-traffic-treatment noquota buffer
        pending-traffic-treatment quota-exhausted buffer
        exit
    exit
context <context_name>
    subscriber default
        ip access-group <acl_name> in
        ip access-group <acl_name> out
        ip context-name <context_name>
        active-charging rulebase <rulebase_name>
        credit-control-group <cc_group_name>
        end
```

Notes:

- For information on configuring IP access lists, refer to the *Access Control Lists* chapter in the *Cisco ASR 5000 Series Systems Administration Guide*.
- For more information on configuring ECS ruledefs, refer to the *ACS Ruledef Configuration Mode Commands* chapter in the *Cisco ASR 5000 Series Command Line Interface Reference*.
- For more information on configuring ECS charging actions, refer to the *ACS Charging Action Configuration Mode Commands* chapter in the *Cisco ASR 5000 Series Command Line Interface Reference*.
- For more information on configuring ECS rulebases, refer to the *ACS Rulebase Configuration Mode Commands* chapter in the *Cisco ASR 5000 Series Command Line Interface Reference*.

Gathering Statistics

This section explains how to gather Gy and related statistics and configuration information.

In the following table, the first column lists what statistics to gather, and the second column lists the action to perform.

Statistics/Information	Action to perform
Complete statistics for ECS sessions.	**show active-charging sessions full**
Information on all rule definitions configured in the service.	**show active-charging ruledef all**
Information on all charging actions configured in the service.	**show active-charging charging-action all**
Information on all rulebases configured in the service.	**show active-charging rulebase all**
Statistics of the Credit Control application, DCCA.	**show active-charging credit-control statistics**
States of the Credit Control application's sessions, DCCA.	**show active-charging credit-control session-states [rulebase** <*rulebase_name*> **] [content-id** <*content_id*> **]**

Appendix D
ICAP Interface Support

This chapter provides information on configuring the external Active Content Filtering servers for a core network service subscriber. This chapter also describes the configuration and commands that are used to implement this feature.

It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in respective product Administration Guide, before using the procedures in this chapter.

Supported Networks and Platforms

This feature supports ST16 and Cisco® ASR 5000 Chassis for the core network services configured on the system.

Licensing

External Content Filtering Server support through Internet Content Adaptation Protocol (ICAP) interface is a licensed feature.

To enable this feature on your chassis you must install one of the following licenses, along with other required core network and in-line service licenses:

- Cisco PID [ASR5K-00-CS01ICAP] *Content Filtering ICAP Interface, 1K sessions*, or Starent Part Number [600-00-7578] *Content Filtering ICAP Interface, 1K sessions*.
- Cisco PID [ASR5K-00-CS10ICAP] *Content Filtering ICAP Interface, 10K Sessions*, or Starent Part Number [600-00-8530] *Content Filtering ICAP Interface, 10K Sessions*.

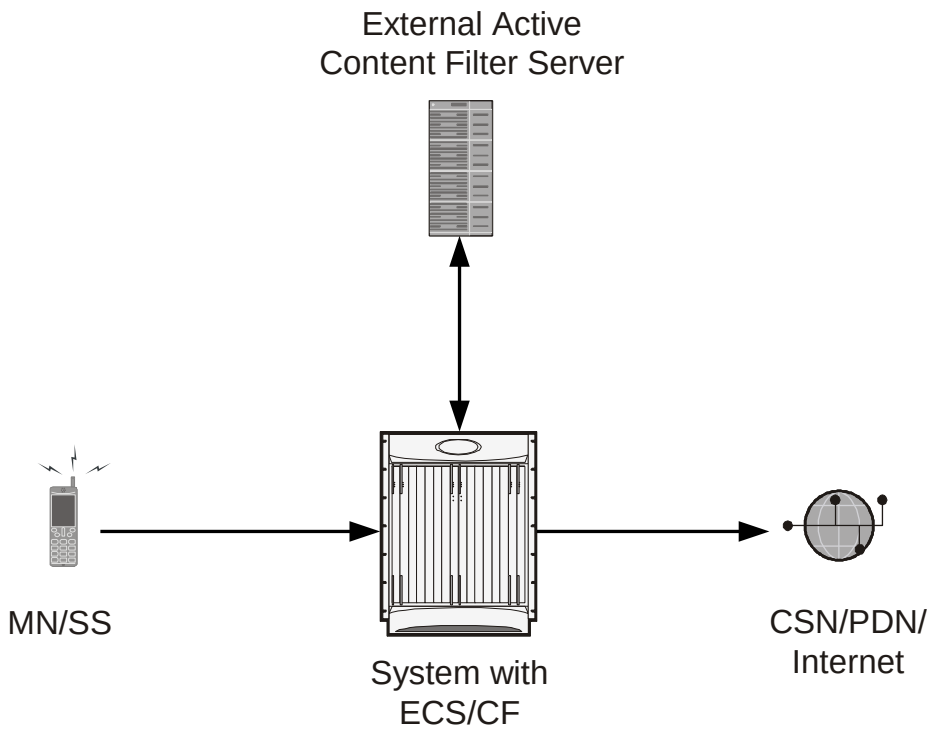
For information on obtaining and installing licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *Cisco ASR 5000 Series System Administration Guide*.

ICAP Interface Support Overview

This feature supports streamlined ICAP interface to leverage Deep Packet Inspection (DPI) to enable external application servers to provide their services without performing DPI, and without being inserted in the data flow. For example with an external Active Content Filtering (ACF) Platform.

A high-level view of the streamlined ICAP interface support for external ACF is shown in the following figure:

Figure 18. High-Level View of Streamlined ICAP Interface with external ACF



The system with ECS is configured to support DPI and the system uses this capability for content charging as well.

If a subscriber initiates a WAP (WAP1.x or WAP2.0) or Web session, the subsequent GET/POST request is detected by the DPI function. The URL of the GET/POST request is extracted and passed, along with subscriber identification information and the subscriber request, in an ICAP message to the application server. The application server checks the URL on the basis of its category and other classifications like, type, access level, content category and decides if the request should be authorized, blocked, or redirected by answering to the GET/POST with:

- A 200 OK message if the request is accepted
- A 302 Redirect message in case of redirection. This redirect message includes the URL to which the subscriber should be redirected
- A 403 Denied message is the request should be blocked

Depending on the response received, the system with ECS will either pass the request unmodified, or discard the message and respond to the subscriber with the appropriate redirection or block message.

Content charging is performed by the Active Charging Service (ACS) only after the request has been controlled by the application server. This guarantees the appropriate interworking between the external application and content-based billing. In particular, this guarantees that charging will be applied to the appropriate request in case of redirection, and that potential charging-based redirections (i.e. Advice of Charge, Top Up page, etc.) will not interfere with the decisions taken by the application server.

Functions of the ACF include:

- Retrieval of subscriber policies based on the subscriber identity passed in the ICAP message
- Determining the appropriate action (permit, deny, redirect) to take for the type of content based on subscriber profile
- Communication of the action (permit, deny, or redirect) decision for the URL back to the ACS module

Failure Action on Retransmitted Packets

ICAP rating is enabled for retransmitted packet when default ICAP failure action was taken on an ICAP request for that flow. ICAP default failure action is taken on the pending ICAP request for a connection when the connection needs to be reset and there is no other redundant connection available. For example, in the ICAP request timeout and ICAP connection timeout scenarios. In these cases the retransmitted packet in the uplink direction is sent for ICAP rating again.

In case of WAP CO, uplink retransmitted packet for the WAP transactions for which ICAP failure action was taken will be sent for ICAP rating. WSP header of the retransmitted packet is not parsed by the WSP analyzer. The URL received in the previous packet for that transaction is used for ICAP rating. If failure action was taken on multiple WTP transactions for the same flow (case: WTP concatenated GET request) then uplink retransmitted packet for each of the transaction is sent for rating again.

In case of HTTP, uplink retransmitted packets for the HTTP flow on which ICAP failure action is taken is sent for ICAP rating. The URL present in the current secondary session (last uplink request) is used for ICAP rating. However, if there were multiple outstanding ICAP request for the same flow (pipelined request) then for the retransmitted packet the URL that will be sent for rating will be that of the last GET request.

Retransmission in various cases of failure-action taken on re-transmitted packets when the ICAP response is not received for the original request and the retransmitted request comes in:

- WSP CO:
    - Permit: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed/blocked. It is possible that the WAP gateway sends the response for the permitted GET request. Hence, there is a race condition and the subscriber may be able to view the web page even thought the rating was redirect or content insert.
    - Content Insert: The retransmitted packet is not sent for ICAP rating.
    - Redirect: The retransmitted packet is not sent for ICAP rating.
    - Discard: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed/blocked.
    - Terminate flow: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed or blocked. The WAP gateway may send an Abort transaction for this GET request if the WSP disconnect packet sent while terminating the flow is received by the WAP gateway.

- HTTP:
  - Permit: The uplink packet is sent for ICAP rating and depending on the ICAP response the last HTTP GET request. It is possible that the HTTP server sends the response for the permitted GET request. Hence there is a race condition and the subscriber may be able to view the web page even thought the rating was redirect or content insert.
  - Content Insert: Retransmitted packets are dropped and not charged.
  - Redirect: Retransmitted packets are dropped and not charged.
  - Discard: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction allowed/blocked.
  - Terminate flow: Retransmitted packets are dropped and not charged.

Configuring ICAP Interface Support

This section describes how to configure the Content Filtering Server Group (CFSG) through Internet Content Adaptation Protocol (ICAP) interface between ICAP client and ACF server (ICAP server).

Important: This section provides the minimum instruction set for configuring external content filtering servers on ICAP interface on the system. For more information on commands that configure additional parameters and options, refer to *CFSG Configuration Mode Commands* chapter in *Cisco ASR 5000 Series Command Line Interface Reference*.

To configure the system to provide ICAP interface support for external content filtering servers:

Step 1 Create the Content Filtering Server Group and create ICAP interface with origin (local) IP address of chassis by applying the example configuration in the Creating ICAP Server Group and Address Binding section.

Step 2 Specify the active content filtering server (ICAP sever) IP addresses and configure other parameters for ICAP server group by applying the example configuration in the Configuring ICAP Server and Other Parameters section.

Step 3 Configure the content filtering mode to external content filtering server group mode in ECS rule base by applying the example configuration in the Configuring ECS Rulebase for ICAP Server Group section.

Step 4 *Optional*. Configure the charging action to forward HTTP/WAP GET request to external content filtering servers on ICAP interface in Active Charging Configuration mode by applying the example configuration in the Configuring Charging Action for ICAP Server Group section.

Step 5 Verify your ICAP interface and external content filtering server group configuration by following the steps in the Verifying the ICAP Server Group Configuration section.

Step 6 Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Creating ICAP Server Group and Address Binding

Use the following example to create the ICAP server group and bind the IP addresses:

```
configure
   context <icap_ctxt_name> [ -noconfirm ]
      content-filtering server-group <icap_svr_grp_name> [ -noconfirm ]
         origin address <ip_address>
         end
```

Notes:

- *<ip_address>* is local IP address of the CFSG endpoint.

Configuring ICAP Server and Other Parameters

Use the following example to configure the active content filtering (ICAP server) and other related parameters:

```
configure

   context <icap_context_name>

      content-filtering server-group <icap_server_grp_name>

         icap server <ip_address> [ port <port_number>][max <max_msgs>][priority
<priority>]

         deny-message <msg_string>

         response-timeout <timeout>

         connection retry-timeout <retry_timeout>

         failure-action { allow | content-insertion <content_string> | discard |
redirect-url <url> | terminate-flow }

         dictionary {custom1 | custom2 | standard}

         end
```

Notes:

- In StarOS 8.1 and later, a maximum of five ICAP servers can be configured per Content Filtering Server Group. In StarOS 8.0, only one ICAP Server can be configured per Content Filtering Server Group.
- The maximum outstanding request per ICAP connection configured using the optional **max** *<max_msgs>* keyword is limited to one. Therefore, any other value configured using the **max** keyword will be ignored.
- *Optional*. To configure the ICAP URL extraction behavior, in the Content Filtering Server Group configuration mode, enter the following command:

  url-extraction { after-parsing | raw }

  By default, percent-encoded hex characters in URLs sent from the ACF client to the ICAP server will be converted to corresponding ASCII characters and sent.

Configuring ECS Rulebase for ICAP Server Group

Use the following example to configure the content filtering mode to ICAP server mode in the ECS rulebase for content filtering:

```
configure
   require active-charging [optimized-mode]
   active-charging service <acs_svc_name> [-noconfirm]
      rulebase <rulebase_name> [-noconfirm]
         content-filtering mode server-group <cf_server_group>
         end
```

Notes:

- In StarOS 8.1, the **optimized-mode** keyword enables ACS in the Optimized mode, wherein ACS functionality is managed by SessMgrs. In StarOS 8.1, ACS must be enabled in the Optimized mode.
- In StarOS 8.3, the **optimized-mode** keyword is obsolete. With or without this keyword ACS is always enabled in Optimized mode.
- In StarOS 8.0 and StarOS 9.0 and later, the **optimized-mode** keyword is not available.

Configuring Charging Action for ICAP Server Group

Use the following example to configure the charging action to forward HTTP/WAP GET request to ICAP server for content processing:

```
configure
   active-charging service <acs_svc_name>
      charging-action <charging_action_name> [ -noconfirm ]
         content-filtering processing server-group
         end
```

Verifying the ICAP Server Group Configuration

This section explains how to display and review the configurations after saving them in a .cfg file as described in *Verifying and Saving Your Configuration* chapter of this guide and also to retrieve errors and warnings within an active configuration for a service.

Important: All commands listed here are under Exec mode. Not all commands are available on all platforms.

These instructions are used to verify the configuration for this feature.

Step 1 Verify your ICAP Content Filtering Server Group configuration by entering the following command in Exec Mode:

`show content-filtering server-group`

The following is a sample output. In this example, an ICAP Content Filtering server group named *`icap_cfsg1`* was configured.

```
Content Filtering Group:     icap_cfsg1

  Context:                     icap1

  Origin Address:              1.2.3.4

  ICAP Address(Port):          1.2.3.4(1344)

  Max Outstanding:             256

  Priority:                    1

  Response Timeout:      30(secs)      Connection Retry
Timeout:      30(secs)

  Dictionary:                   standard

  Timeout Action:               terminate-flow

  Deny Message:                 "Service Not Subscribed"

  URL-extraction:                after-parsing

  Content Filtering Group Connections: NONE

Total content filtering groups matching specified criteria:  1
```

Step 2 Verify any configuration error in your configuration by entering the following command in Exec Mode:

`show configuration errors`

Appendix E
Pre-paid Billing

This chapter provides information on configuring an enhanced, or extended, service. The product administration guides provides examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model and configure the required elements for that model before using the procedures in this chapter.

This chapter includes the following topics:

Overview

The system supports pre-paid billing for subscriber accounts that use RADIUS Accounting. 3GPP2 pre-paid billing support is disabled by default and you must obtain and install a license key to enable it.

The system supports two methods of implementing Pre-paid Billing Support; Standard 3GPP2 Pre-paid Billing and Custom Pre-paid Billing. The 3GPP2 standard is the recommended implementation.

3GPP2 Standard Pre-paid Billing Overview

The prepaid packet data service allows a user to purchase access to the network in advance, based on either volume or duration. When a user connects to a service, the Prepaid Client (PPC) contacts the Prepaid Server (PPS) and verifies that the user has available credits for the service. When a user runs out of credits, service is terminated until the user purchases additional credits.

The Prepaid Data Service implementation is compliant with 3GPP2 IS-835-C. This solution provides a standards based implementation that can effectively interoperate with additional vendors equipment when required. The system primarily uses the PPAC (PrePaid Accounting Capability) and PPAQ (PrePaid Accounting Quota) VSAs to implement PrePaid service. The PPAC VSA is used to determine the capabilities of the PPC. When the PPC sends the PPAC VSA it specifies if it supports duration, volume or both types of PrePaid service. When the PPS sends a PPAC VSA it specifies the type of PrePaid service to use for the particular session. The PPAQ VSA specifies the characteristics of the PrePaid accounting service. This includes quota & threshold values for both duration and volume PrePaid service. Through the use of these VSAs, the PPC and PPS communicate the status of the session and when the user has run out of quota, the service can be terminated.

The PrePaid Client resides on the system and communicates with the PPS through the use of RADIUS messages exchanged with the RADIUS server.

Custom Pre-paid Billing Overview

In the Access-Accept from the RADIUS server the system receives attributes which indicate the number of byte credits available for the subscriber. Byte throughput can be pre-paid for traffic inbound to the system, outbound from the system, or an amount that combines both inbound and outbound traffic. Five attributes are used: one for traffic inbound to the system, one for traffic outbound from the system, one that combines traffic in both directions, one that only indicates that the user should be re-authenticated regardless of the byte counters, and one for the low watermark in percent.

The low watermark value is multiplied by the number of byte credits granted in the Access-Accept to arrive at a threshold. Once the number of byte credits remaining is lower than this number, a new Access-Request is issued. If the Access-Request is issued because the Low Watermark has been reached, then a new Low Watermark is calculated from the number of byte credits granted in the Access-Accept, but only if the number of byte credits granted is a non-zero value. If the Access-Request is issued for any other reason, then the Low Watermark is not re-calculated.

The system re-authorizes an active subscriber that has used up its byte credits by issuing a RADIUS Access-Request to the RADIUS server. A valid Access-Reject or a RADIUS timeout results in immediate disconnect of the subscriber session. An Access-Accept without attributes that authorize more byte credits allows the subscriber session to continue with the remaining credits. An Access-Accept with attributes containing byte credits results in the addition of these byte

credits to the subscriber session, and the continuation of the session until the subscriber session byte credits have been reduced to the low watermark received in the access accept. If not received, it defaults to 10%.

The system continues to service the subscriber session while the RADIUS request for re-authorization is in process. If the counter reaches zero before the response the subscriber session is terminated immediately.

You can configure Pre-paid Billing support for standard 3GPP2 behavior or custom behavior where you can specify whether or to measure the bye-count on compressed or non-compressed data, set a low-watermark for accounting, and specify a credit renewal interval in the default subscriber configuration for a context or a domain alias.

Licensing

This feature requires the following license to be installed on the chassis:

- Cisco PID [ASR5K-00-CS01PPAC] *Prepaid Accounting with countdown, 1K sessions*, or Starent Part Number [600-00-7509] *Prepaid Accounting*.
- Cisco PID [ASR5K-00-CSXXPPD] *Standard IS-835C Prepaid Bundle*, or Starent Part Number [600-00-7561] *IS-835C Prepaid Bundle*.

For information on obtaining and installing licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Configuring Standard 3GPP2 Pre-paid Billing

This section describes how to enable standard 3GPP2 pre-paid billing support.

Important: Commands used in the configuration samples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

Enable pre-paid billing for the default subscriber by applying the following example configuration:

```
configure
   context <context_name>
      subscriber default
         prepaid 3gpp2 accounting
         end
```

Enable pre-paid billing for the default subscriber of a domain alias by applying the following example configuration:

```
configure
   context <context_name>
      subscriber name <alias_def_sub>
         prepaid 3gpp2 accounting
         end
```

Notes:

- You may add the optional keyword **`no-final-access-request`** to the **`prepaid 3gpp2 accounting`** command to stop sending the final online access-request on termination of 3GPP2 prepaid sessions.
- Optional commands: If both duration and volume attributes are received, default preference is given to the duration attribute. To set the preference to the volume attribute, enter the following command:

  `prepaid 3gpp2 preference volume`

  Note that this command alone does not enable pre-paid support. The **`prepaid 3gpp2 accounting`** command must be executed as shown to enable pre-paid support.

  If you are using duration-based quota usage accounting, use the following command to define what behavior specifies the end of the billing duration. The default behavior is the duration quota algorithm set to current-time.

  `prepaid 3gpp2 duration-quota final-duration-algorithm [ current-time | last-airlink-activity-time | last-user-layer3-activity-time ]`

  Note that this command alone does not enable pre-paid support. The **`prepaid 3gpp2 accounting`** command must be executed as shown to enable pre-paid support.

Save the configuration as described in the *Verifying and Saving Your Configuration* chapter.

Configuring Pre-paid Billing With Custom Behavior

This section describes how to enable Pre-paid billing support with custom behavior.

Important: If RADIUS attributes are present that conflict with the custom pre-paid settings, the values set by the RADIUS attributes take precedence.

Important: Pre-paid billing support is not available for local subscribers. Even though you can set pre-paid parameters for a local subscriber from the CLI, these settings have no effect on a subscriber session.

Important: Commands used in the configuration samples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

Enable custom pre-paid billing for the default subscriber by applying the following example configuration:

```
configure
   context <context_name>
      subscriber default
         prepaid custom
         end
```

Enable custom pre-paid billing for the default subscriber of a domain alias by applying the following example configuration:

```
configure
   context <context_name>
      subscriber name <alias_def_sub>
         prepaid custom
         end
```

Notes:

- *Optional*: To have custom pre-paid byte credits based on the flow of compressed traffic, use the following command:

  prepaid custom byte-count compressed

- *Optional*: Set the low-watermark for remaining byte credits. This is a percentage of the subscriber session's total credits. When the low-watermark is reached a new RADIUS access-request is sent to the RADIUS server to retrieve more credits. To set the low watermark percentage, enter the following command:

prepaid custom low-watermark percent *<percentage>*

- *Optional*: Set the time in seconds to wait before sending a new RADIUS access-request to the RADIUS server to retrieve more credits by entering the following command:

  prepaid custom renewal interval *<seconds>*

- Save the configuration as described in the *Verifying and Saving Your Configuration* chapter.

3GPP2 Pre-paid Attributes

Use the attributes listed in the following table to configure a subscriber for 3GPP2 pre-paid billing;

Attribute	Sub-attribute	Description
3GPP2-Pre-Paid-Acct-Capability		This attribute is for setting the prepaid accounting capability.
	Available-In-Client	The optional Available-In-Client Sub-Type, generated by the PrePaid client, indicates the PrePaid Accounting capabilities of the client in the PDSN or HA and shall be bitmap encoded.
	Selected-For-Session	The optional Selected-For-Session Sub-Type, generated by the PrePaid server, indicates the PrePaid Accounting capability to be used for a given session.
3GPP2-Pre-Paid-Accounting-Quota		This attribute specifies the characteristics for PrePaid accounting of the volume and/or duration of a packet data session. It shall be present in all on-line RADIUS Access-Request and on-line RADIUS Access-Accept messages and may be included in other RADIUS Access-Accept messages. Non-used Sub-Types by the PPC and PPS shall be omitted.
	Quota-Identifier	The Quota-Identifier Sub-Type is generated by the PrePaid server at allocation of a Volume and/or Duration Quota. The on-line quota update RADIUS Access-Request message sent from the PPC to the PPS shall include a previously received Quota-Identifier.
	Volume-Quota	The optional Volume-Quota Sub-Type is only present if Volume Based charging is used. In RADIUS Access-Accept message (PPS to PPC direction), it indicates the Volume (in octets) allocated for the session by the PrePaid server. In on-line RADIUS Access-Request message (PPC to PPS direction), it indicates the total used volume (in octets) for both forward and reverse traffic applicable to PrePaid accounting13. If a Tariff Switch condition was reached during the session, this Sub-Type contains the complete (before and after) volume used, while the Volume-Used-After-Tariff-Switch attribute contains the volume used after the tariff switch condition.
	Volume-Quota-Overflow	The optional Volume-Quota-Overflow Sub-Type is used to indicate how many times the Volume-Quota counter has wrapped around 2^32 over the course of the service being provided.
	Volume-Threshold	The Volume-Threshold Sub-Type shall always be present if Volume-Quota is present in a RADIUS Access-Accept message (PPS to PPC direction). It is generated by the PrePaid server and indicates the volume (in octets) that shall be used before requesting quota update. This threshold should not be larger than the Volume-Quota.
	Volume-Threshold-Overflow	The optional Volume-Threshold-Overflow Sub-Type is used to indicate how many times the Volume-Threshold counter has wrapped around 2^32 over the course of the service being provided.
	Duration-Quota	The optional Duration-Quota Sub-Type is only present if Duration Based charging is used. In RADIUS Access-Accept message (PPS to PPC direction), it indicates the Duration (in seconds) allocated for the session by the PrePaid server. In on-line RADIUS Access-Accept message (PPC to PPS direction), it indicates the total Duration (in seconds) since the start of the accounting session related to the Quota-ID.

Attribute	Sub-attribute	Description
	Duration-Threshold	The Duration-Threshold Sub-Type shall always be present if Duration-Quota is present in a RADIUS Access-Accept message (PPS to PPC direction). It represents the duration (in seconds) that shall be used by the session before requesting quota update. This threshold should not be larger than the Duration-Quota and shall always be sent with the Duration-Quota.
	Update-Reason	The Update-Reason Sub-Type shall be present in the on-line RADIUS Access-Request message (PPC to PPS direction). It indicates the reason for initiating the on-line quota update operation. Update reasons 4, 5, 6, 7 and 8 indicate that the associated resources are released at the client side, and therefore the PPS shall not allocate a new quota in the RADIUS Access-Accept message.
	Pre-Paid-Server	The optional, multi-value PrePaid-Server indicates the address of the serving PrePaid System. If present, the Home RADIUS server uses this address to route the message to the serving PrePaid Server. The attribute may be sent by the Home RADIUS server. If present in the incoming RADIUS Access-Accept message, the PDSN shall send this attribute back without modifying it in the subsequent RADIUS Access-Request message, except for the first one. If multiple values are present, the PDSN shall not change the order of the attributes.

These attributes can be found in the following dictionaries:

- 3gpp2
- 3gpp2-835
- starent
- starent-835
- starent-vsa1
- starent-vsa1-835

For more information, refer to the *AAA and GTPP Interface Administration and Reference*.

Pre-paid Attributes

Use the attributes listed in the following table to configure a subscriber for pre-paid billing;

Attribute	Description
SN-Prepaid-Inbound-Octets	If only SN-Prepaid-Inbound-Octets is in the Access-Accept, and the others are not, then the number of outbound credits is infinite.
SN-Prepaid-Outbound-Octets	If only SN-Prepaid-Outbound-Octets is in the Access-Accept, and the others are not, then the number of inbound credits is infinite.
SN-Prepaid-Total-Octets	If only SN-Prepaid-Total-Octets is in the Access-Accept, and the others are not, then pre-paid credits is only enforced on the total byte throughput.
SN-Prepaid-Timeout	SN-Prepaid-Timeout can be used alone or in combination with the other attributes. This integer RADIUS attribute includes a time limit in seconds. Regardless of the values of the Octet counters, the session should send a new authorization request upon timer expiration.
SN-Prepaid-Watermark	SN-Prepaid-Watermark is optional with any of the attributes. If it is not included it defaults to the CLI default subscriber configuration, which defaults to a value of 10%. This watermark applies to any of the pre-paid attributes being enforced.

These attributes can be found in the following dictionaries:

- starent
- starent-vsa1
- starent-835
- starent-vsa1-835
- custom1 through custom9

Refer to the *AAA and GTPP Interface Administration and Reference* for more details.

Appendix F
IP Services Gateway Engineering Rules

This appendix lists IPSG-specific engineering rules that must be considered prior to configuring the system for your network deployment. General and network-specific rules are available in the appendix of the *System Administration Guide* for the specific network type.

The following rules are covered in this appendix:

IPSG Context and Service Rules

- Only one IPSG service can be configured within a context.
- Single context configurations must have the ingress port identified using the **ingress-mode** command in the Ethernet Port Configuration Mode.
- In single context configurations, if data packets are received before a session is initiated, the packets could be routed to their destination without being processed. Use separate ingress and egress contexts to prevent this issue.

IPSG RADIUS Messaging Rules

- The sending of RADIUS accounting start messages to the RADIUS server is delayed by the IPSG until a session is successfully started.