IPSG Administration Guide, StarOS Release 21.23

First Published: 2021-03-31

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

CONTENTS

About this Guide

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Note The HA, HSGW, PDSN, and SecGW products have reached end of life and are not supported in this release. Any references to these products (specific or implied) their components or functions including CLI commands and parameters in this document are coincidental and are not supported. Full details on the end of life for these products are available at https://www.cisco.com/c/en/us/products/collateral/wireless/asr-5000-series/eos-eol-notice-c51-740422.html.

This preface describes the *IPSG Administration Guide*, how it is organized, and its document conventions.

The IP Services Gateway (IPSG) is a StarOS™ application that runs on Cisco® ASR 5500 and virtualized platforms.

- Conventions Used, on page xiii
- Supported Documents and Resources, on page xv

Conventions Used

The following tables describe the conventions used throughout this documentation.

Notice Type	Description
Information Note	Provides information about important features or instructions.
Caution	Alerts you of potential damage to a program, device, or system.

Notice Type	Description
Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.

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 keyword options and variables are those components that are required to be entered as part of the command syntax. Required keyword options and variables are surrounded by grouped braces { }. For example: **sctp-max-data-chunks { limit** *max_chunks* **| mtu-limit }** If a keyword or variable is not enclosed in braces or brackets, it is mandatory. For example: **snmp trap link-status**
[keyword or *variable* **]**	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by brackets.

Command Syntax Conventions	Description
|	Some commands support multiple options. These are documented within braces or brackets by separating each option with a vertical bar. These options can be used in conjunction with required or optional keywords or variables. For example: **action activate-flow-detection { intitiation | termination }** or **ip address [count** *number_of_packets* **| size** *number_of_bytes* **]**

Supported Documents and Resources

Related Common Documentation

The most up-to-date information for this product is available in the product Release Notes provided with each product release.

The following common documents are available:

- *AAA Interface Administration and Reference*
- *Command Line Interface Reference*
- *GTPP Interface Administration and Reference*
- *Installation Guide* (hardware dependent)
- *VPC-SI System Administration Guide*
- *Release Change Reference*
- *SNMP MIB Reference*
- *Statistics and Counters Reference*
- *System Administration Guide* (hardware dependent)
- *Thresholding Configuration Guide*

Related Product Documentation

The following product documents are also available and work in conjunction with IPSG:

- *ADC Administration Guide*
- *ECS Administration Guide*
- *GGSN Administration Guide*
- *P-GW Administration Guide*

Obtaining Documentation

The most current Cisco documentation is available on the following website:

http://www.cisco.com/cisco/web/psa/default.html

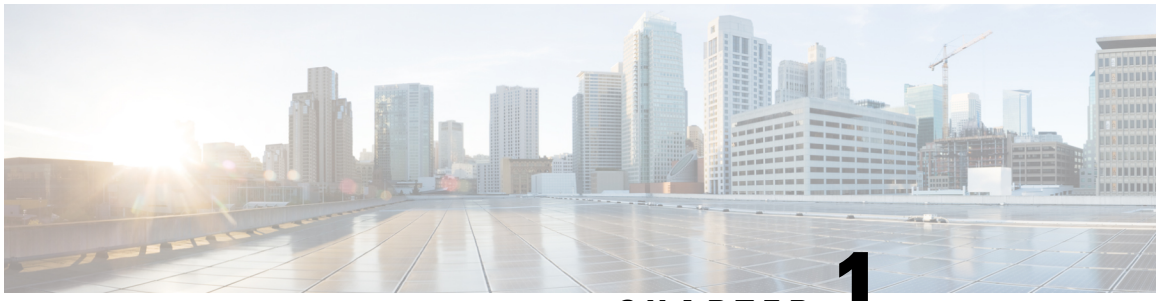
Use the following path selections to access the IPSG documentation:

Products > Wireless > Mobile Internet> Network Functions > Cisco IPSG IP Services

Contacting Customer Support

Use the information in this section to contact customer support.

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 are required to access this site. Please contact your Cisco sales or service representative for additional information.



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.

IPSG only requires a RADIUS request (access and accounting messages) with all the required mandatory attributes to create a session. Currently, IPSG supports GGSN (2G, 3G), PDSN, HA, Broadband Remote Access Server (B-RAS). IPSG does not support the radio access types (RAT) of 4G (EUTRAN) and Wi-Fi and hence cannot be deployed with P-GW (with 4G, Wi-Fi access, 2G/3G SGSN based RATs).

Important Pre StarOS Release 21.3, IPSG supported only for 3G RAT type. From StarOS Release 21.3, 4G RAT Type and EPS QoS is supported. Support has been extended for IPSG to operate in the 4G RAT environment which enables IPSG to act as an inline service agent in the core 4G network.

For the list of AAA attributes supported by IPSG, refer to the *IP Services Gateway AAA AVP Support* appendix.

Qualified Platforms

IPSG is a StarOS™ application that runs on Cisco® ASR 5500 and virtualized platforms. For additional platform information, refer to the appropriate *System Administration Guide* and/or contact your Cisco account representative.

License Requirements

The IP Services Gateway is a licensed Cisco product. Separate session and feature licenses may be required. Contact your Cisco account representative for detailed information on licensing requirements.

For information on installing and verifying 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:

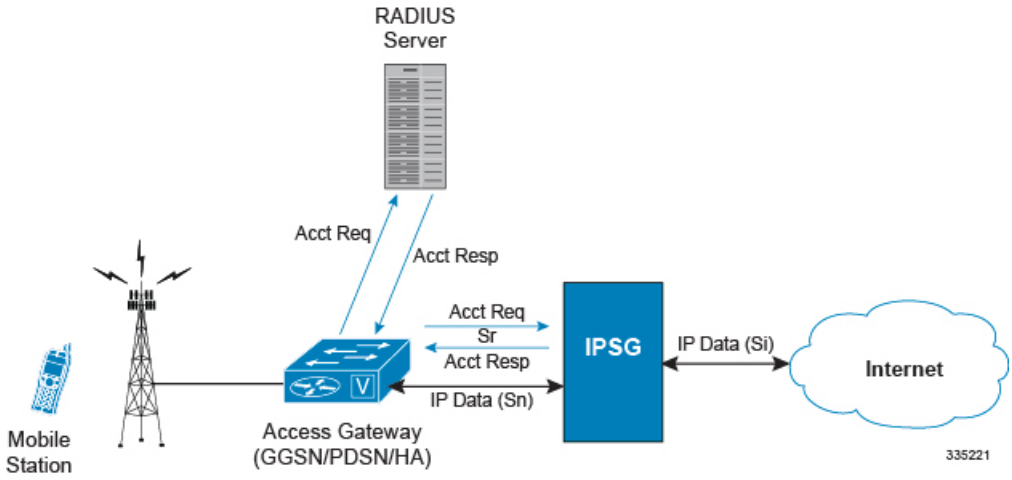
- RADIUS Server Mode, on page 2
- RADIUS Snoop Mode, on page 3

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.

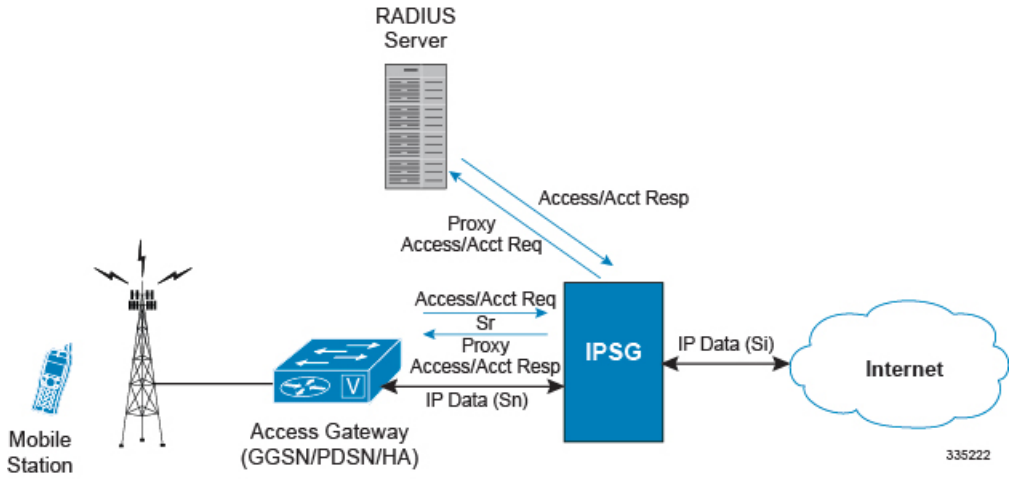
Figure 1: IPSG Message/Data Flow (RADIUS Server Mode)



RADIUS Proxy

In the event that the Access Gateway is incapable of sending two separate RADIUS Start messages, 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)

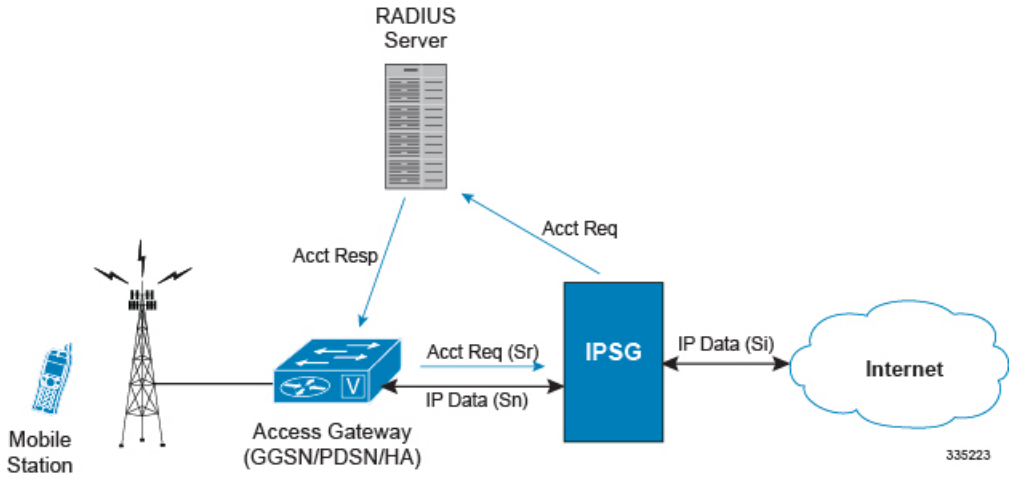


RADIUS Snoop Mode

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.

Accounting-On and Accounting-Off Messages

This feature introduces IPSG support for Accounting-On and Accounting-Off RADIUS accounting messages, in addition to the existing start, interim-update, and stop messages. The Accounting-On message sent by the peer RADIUS client indicates that the RADIUS client has restarted and is ready to accept calls.

An Accounting-Off message indicates that the peer RADIUS client is shutting down.

IPSG clears the existing subscriber sessions on receiving the Accounting-On/Off messages, and proxies the message to the RADIUS server (Proxy mode). The existing sessions are cleared based on the NAS-IP address of the subscriber that was assigned when the Acct-start message was created . If there is no NAS-IP-Address available, the peer IP address is considered as the NAS-IP-Address for the session. IPSG clears calls based on the NAS-IP address AVP in the Accounting-On/Off message irrespective of the origin of the message.

IPSG Server Mode

In the server mode, IPSG acts like the RADIUS server and on receiving an Accounting-On message, IPSG clears the existing sessions based on the NAS-IP address and sends a response to the RADIUS client.

When an Accounting-Off message is received, IPSG clears the existing sessions mapped to that NAS-IP address and sends a response to the client.

Only the first Accounting-On/Off message from the RADIUS client is addressed and the sessions are not cleared for retries. However, a response is sent to the RADIUS client for the retries.

IPSG Proxy Mode

In the proxy mode, when IPSG receives the Accounting-On/Off message from the RADIUS client, IPSG clears the subscriber sessions based on the NAS-IP address and proxies the message to the RADIUS server. IPSG then proxies the response from the RADIUS server back to the RADIUS client. Only the first Accounting-On/Off message from the RADIUS client is addressed. The corresponding messages are proxied directly to the RADIUS server and the response proxied back to the RADIUS client.

Cisco Ultra Traffic Optimization

In a high-bandwidth bulk data flow scenario, user experience is impacted due to various wireless network conditions and policies like shaping, throttling, and other bottlenecks that induce congestion, especially in the RAN. This results in TCP applying its saw-tooth algorithm for congestion control and impacts user experience, and overall system capacity is not fully utilized.

The Cisco Ultra Traffic Optimization solution provides clientless optimization of TCP and HTTP traffic. This solution is integrated with Cisco IPSG and has the following benefits:

- Increases the capacity of existing cell sites and therefore, enables more traffic transmission.
- Improves Quality of Experience (QoE) of users by providing more bits per second.
- Provides instantaneous stabilizing and maximizing per subscriber throughput, particularly during network congestion.

For detailed information on Cisco Ultra Traffic Optimization solution, refer to the *Cisco Ultra Traffic Optimization* chapter in the *IPSG 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 that filtering is required for a subscriber, CSS is 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*.

Dynamic RADIUS Extensions (Change of Authorization)

Dynamic RADIUS extension support provides 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 of this 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).

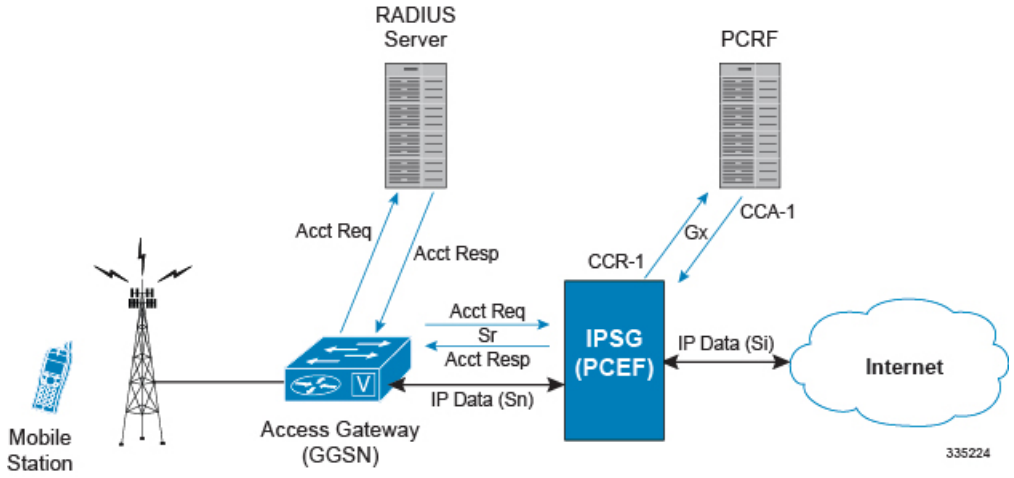
For detailed information on Gx Interface support, refer to the *Gx Interface Support* appendix in the *IP Services Gateway Administration Guide*.

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*.

Lawful Intercept

The Cisco Lawful Intercept feature is supported on the IPSG. Lawful Intercept is a license-enabled, standards-based feature that provides telecommunications service providers with a mechanism to assist law enforcement agencies in monitoring suspicious individuals for potential illegal activity. For additional information and documentation on the Lawful Intercept feature, contact your Cisco account representative.

Multiple IPSG Services

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

Overlapping IP Support over VLAN

Support for overlapping IP addresses for subscribers serviced by access networks on IPSG using VLANs is now possible through this feature. Overlapping IP addresses can be set up by defining multiple interfaces on the Sn interface (access side) and binding them to separate VLANs, while a single interface is setup to separate traffic using VPNv4 on the Si side (network side). When IPSG receives a packet, the appropriate session is identified based on the combination of IP address and VLAN. Currently, a maximum of 500 VLANs can be configured.

IPSG running on Cisco ASR 5500 acts as a BGPv4 peer (BGP proxy) per VLAN on the Sn interface, and MP-BGP peer on the Si interface. There can be 500 BGPv4 peers on the access side. IPSG can support a maximum of 64 BGP sessions per context, and hence 8 contexts are required to address 500 BGP sessions. On the Si interface, one VPNv4 per context is used, with a maximum of 8 VPNv4 contexts (if 8 contexts are used). The Sn and Si interfaces must be in the same context.

The session creation and deletion on IPSG is triggered on receiving the enriched AAA Accounting Start/Stop requests from the Cisco Account Register (CAR) AAA. The VLAN information is forwarded using the SN1-Assigned-VLAN-ID AVP.

This feature can be enabled using the CLI in the IPSG RADIUS Server Configuration Mode. Refer the *IP Services Gateway Configuration* chapter for configuration information.

Call Flows for Overlapping IP Support over VLAN

The following call flow illustration and descriptions explain how a session is created:

Figure 5: Session Creation Call Flow

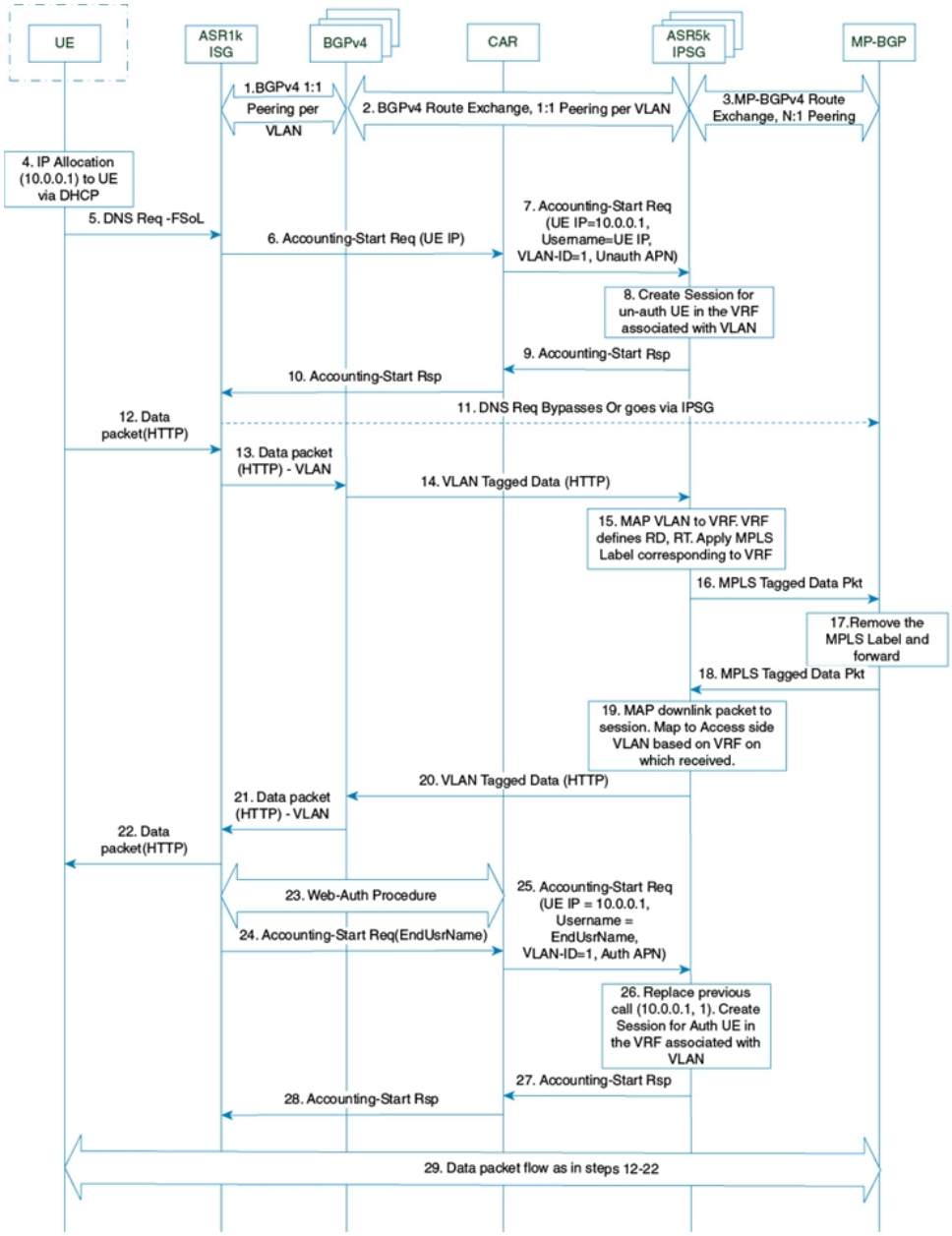


Table 1: Session Creation Call Flow Descriptions

Step	Description
1—3	BGP peering is established and routes exchange between ISG, BGPv4 routers, IPSG and MP-BGP router.

Step	Description
6—10	**Unauthenticated Phase**: In the pre-auth stage, the applicable username and other attributes pertaining to the subscriber are not available. The session creation request (Accounting-Start Req) at IPSG contains Username=UE IP (this should be string type), Framed-IP-Address=UE IP, Calling-Station-Id="000000000000000", 3GPP-IMSI="000000000000000", SN-Assigned-VLAN-ID=VlanId, Called-Station-Id="UnauthEud"; 3GPP-RAT-Type="UTRAN".
12—22	HTTP redirection occurs at IPSG.
23	The user between the ISG and CAR/SIS is authenticated using and user credentials like EndUserName, EndUserId used for 3GPP-IMSI , Calling-Station-id, auth APN to be used etc are obtained.
24—28	ISG/CAR send a new Accounting Start with the actual user credentials obtained from CAR/SIS subsystems. The same IP address and VLAN ID used during the un-phase is used again. The Username, Calling-Station-Id and APN are updated to reflect the actual user credentials. The replacement feature at IPSG based on diff-key is enabled at IPSG so the new session request replaces the earlier one for the same IP and VLAN-ID. Otherwise, ISG/CAR sends an Accounting-Stop for the previous session created for the un-authenticated user before sending the Accounting-Start for the authenticated user.
29	The uplink and downlink data call flow is same as steps 12-22, where the VLAN tagged data on the Sn interface is mapped to the MPLS tagged data on the Si side and vice-versa.

Dictionary Requirements

This section provides AVP requirements for the overlapping IP support over VLAN feature.

The following are the AVPs required, based on dictionaries starent-vsa1 or custom54

AVP	STARENT-VSA1	CUSTOM54	Additional Information
Acct-Status-Type	Mandatory	Mandatory	—

AVP	STARENT-VSA1	CUSTOM54	Additional Information
User-Name	Mandatory	Optional	For custom54, if present, this AVP is used. Otherwise, a default value "void" is used as the username in ipsgmgr.
Calling-Station-Id	Optional	Mandatory	For starent-vsa1, this AVP will be set to null and processed in ipsgmgr.
Framed-Ip-Address	Mandatory	Mandatory	Optional if an IPv6 prefix exists. Optional for Radio Access requests.
Acct-Session-Id	Mandatory	Mandatory	Optional for Radio Access requests.
Called-Station-Id	Mandatory	Mandatory	Optional for Subscriber profile and Radio Access requests.
SN-Assigned-VLAN-ID	Mandatory	Mandatory	This AVP is used to forward the VLAN ID.
SN-Transparent-Data	Optional	Optional	—
SN-Vpn-Name	Mandatory	Mandatory	This AVP is used to forward the VPN name (destination context).

Radius Client IP Validation

This feature enables IPSG to validate RADIUS accounting messages from different configured RADIUS client IP addresses, and forward requests to the session manager.

In an architecture where multiple sites of IPSG and Radius Proxies exist, GGSN forwards RADIUS accounting messages to IPSG through its Radius Proxy. In an event where the Radius Proxy is unreachable, GGSN forwards subsequent messages using the RADIUS Proxy belonging to another site. IPSG updates the RADIUS client IP in the subscriber session, and forwards all control messages from the session manager to the alternate client.

This feature can be enabled using the **validate-client-ip** keyword in the **radius accounting** command under the IPSG RADIUS Server Configuration Mode. By default, the RADIUS client IPs are validated, and can be disabled using the **disable radius accounting validate-client-ip** command.

Session Recovery

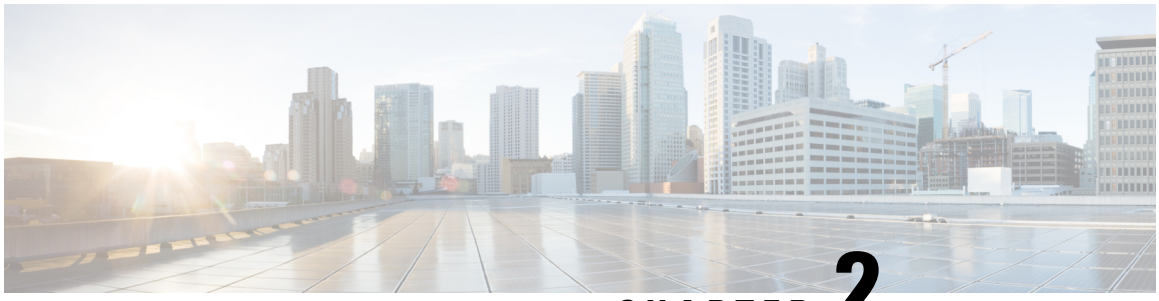
The Session Recovery feature provides seamless failover and reconstruction of subscriber session information in the event of a hardware or software fault within the system preventing a fully connected user session from being disconnected.

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

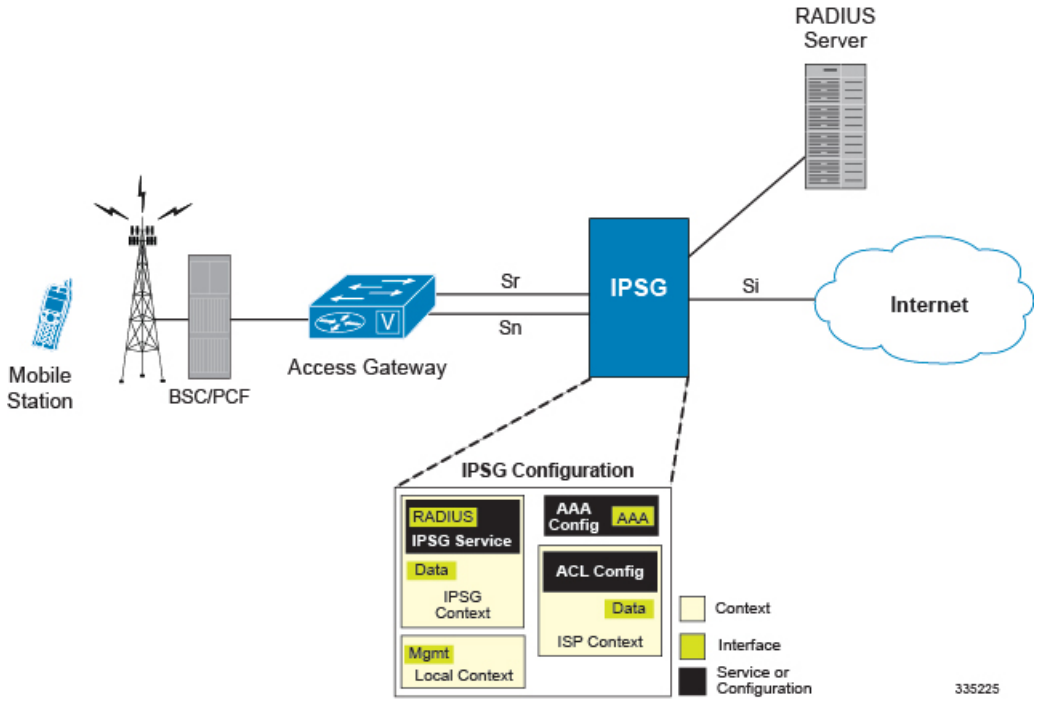
This section provides a high-level description of the configuration requirements of the IPSG.

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 6: 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*.

IPSG RADIUS Dictionaries

The following table provides information on the different IPSG RADIUS dictionaries and the corresponding usage:

Table 2: IPSG RADIUS Dictionaries

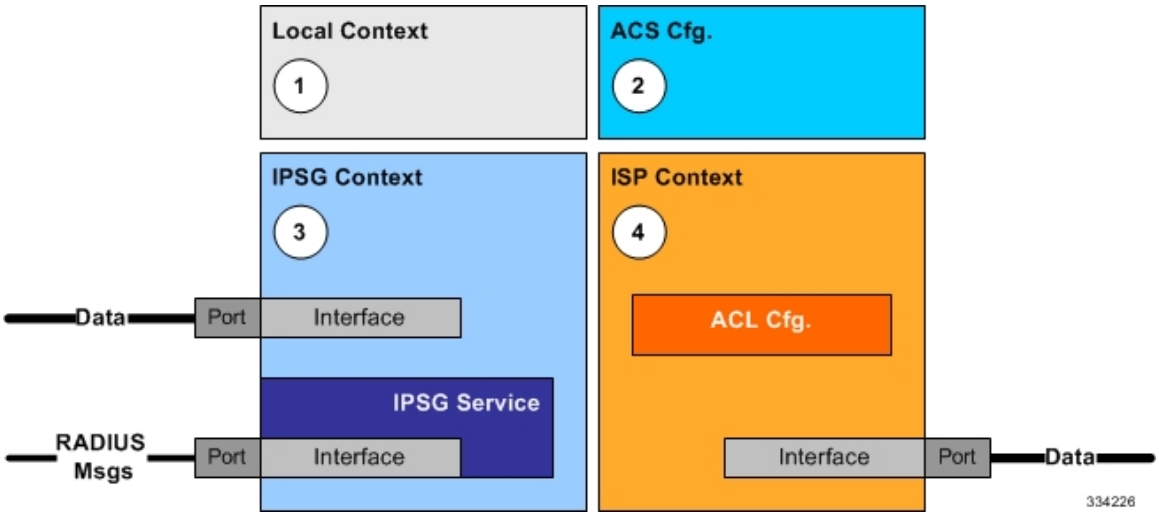
Dictionary	Mandatory Attributes	Session Identity
starent-vsa1	User-Name Acct-Status-Type Acct-Sess-Id Called-Station-Id Framed-IP-Address	User-Name Framed-IP-Address

Dictionary	Mandatory Attributes	Session Identity
custom28	Acct-Status-Type Acct-Sess-Id Called-Station-Id Framed-IP-Address Calling-Station-Id	Calling-station-Id Framed-IP-Address
custom54	Acct-Status-Type Acct-Sess-Id Called-Station-Id Framed-IP-Address Calling-Station-Id	Calling-station-id Framed-IP-Address

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 7: 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 IPSG Context and Service Configuration, on page 17.

Step 4 Configure the Service Provider context by applying the example configuration presented in ISP Context Configuration, on page 19.

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

Step 6 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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, on page 17
- Option 2: RADIUS Server with Proxy Mode Configuration, on page 17
- Option 3: RADIUS Snoop Mode Configuration, on page 18

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 ipsg_service_name mode radius-server
               bind address ipv4/ipv6_address
               radius dictionary dictionary_name
               radius accounting client ipv4/ipv6_address [ encrypted ] key
key [ dictionary dictionary_name ] [ disconnect-message [ dest-port port_number
 ] ]
               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 ipsg_service_name mode radius-server
               bind address ipv4/ipv6_address
               radius dictionary dictionary_name
               radius accounting client ipv4/ipv6_address [ encrypted ] key
key [ dictionary dictionary_name ] [ disconnect-message [ dest-port port_number
 ] ]
# IPSG Authentication Proxy Configuration:
               bind authentication-proxy address ipv4/ipv6_address
               connection authorization [ encrypted ] password password
               radius dictionary dictionary_name
               radius accounting client ipv4/ipv6_address [ encrypted ] key
key [ dictionary dictionary_name ] [ disconnect-message [ dest-port port_number
 ] ]
               exit
          aaa group default
               radius attribute nas-ip-address address ipv4/ipv6_address
               radius dictionary dictionary_name
               radius server ipv4/ipv6_address [ encrypted ] key key port
port_number
               radius accounting server ipv4/ipv6_address [ encrypted ] key
key port port_number
               exit
# IPSG Accounting Proxy Configuration:
          ipsg-service ipsg_service_name mode radius-server
              bind accounting-proxy address ipv4/ipv6_address port port_number

               radius dictionary dictionary_name
               radius accounting client ipv4/ipv6_address [ encrypted ] key
secret_key [ dictionary dictionary_name ] [ disconnect-message [ dest-port
port_number ] ]
               exit
          aaa group default
               radius attribute nas-ip-address address ipv4/ipv6_address
               radius dictionary dictionary_name
               radius accounting server ipv4/ipv6_address [ encrypted ] key
key port port_number
               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 GTP 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 ipsg_service_name mode radius-snoop
               bind
               connection authorization [ encrypted ] password password
               radius accounting server ipv4/ipv6_address
               radius dictionary dictionary_name
               end
```

ISP Context Configuration

To configure the ISP context:

Step 1 Create an ISP context as described in Creating the ISP Context, on page 19.

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_name
               redirect css service css_service_name any
               permit any
               exit
          aaa group default
               exit
          ip route {ipv4_address/mask | ipv6_address } next-hop
next_hop_ipv4/ipv6_address isp_data_interface_name
               end
```

Enhanced and Optional Configurations

This section provides information on enhanced and optional configurations:

Virtual APN Support Configuration

To configure Virtual APN Support use the following configuration:

```
configure
     context ipsg_context_name
          apn apn_name
             virtual-apn preference priority apn apn_name [ access-gw-address
 { ipv4/ipv6_address | ipv4/ipv6_address/mask } | [ msisdn-range { from
msisdn_start_range to msisdn_end_range } ] [ rat-type { eutran | gan | geran |
hspa | utran | wlan } ] ]
               exit
```

RADIUS Server and/or RADIUS Snoop mode

```
          ipsg-service ipsg_service_name mode radius-server
          ipsg-service ipsg_service_name mode radius-snoop
               profile { APN | subscriber }
               end
```

Notes:

- The IPSG Virtual APN feature allows operators to use a single APN to configure differentiated services. The APN selection is based on the APN supplied to the IPSG in conjunction with the following configurable parameters:
  - access-gw-address (for IPSG this means the RADIUS client
  - msisdn-range
  - rat-type
- For more information, refer to the **virtual-apn** CLI command in the *APN Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

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.

Overlapping IP Support over VPN Configuration

To enable Overlapping IP Support over VPN, use the following configuration:

```
config
          context context_name
```

```
ipsg-service ipsg_service_name mode radius-server
     [ default | no ] overlapping-ip-address
end
```

Notes:

- This feature is disabled by default.

Radius Client IP Validation

To enable IPSG to validate RADIUS client IP address, use the following configuration:

```
config
          context context_name
               ipsg-service ipsg_service_name mode radius-server
                    [ default ] radius accounting validate-client-ip
               end
```

Notes:

- This feature is enabled by default.
- Use the **disable radius accounting validate-client-ip** command to disable IPSG from validating the RADIUS client IPs.

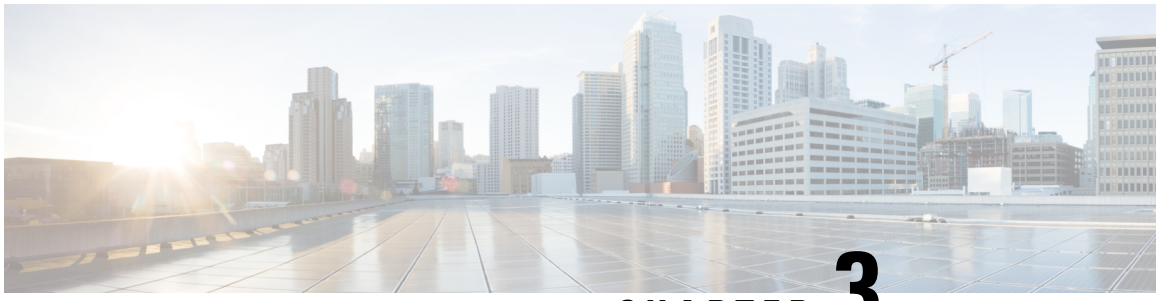
Responding to Accounting-Stop Messages for Non-Existing Sessions

To enable the IPSG service to respond to a RADIUS Accounting-Stop message for a session that does not exist anymore (For example: IPSG service is reset and all active sessions are lost), use the following configuration:

```
config
          context context_name
               ipsg-service ipsg_service_name mode radius-server
                    [ default | no ] respond-to-non-existing-session
               end
```

Notes:

- This feature is disabled by default.



CHAPTER 3

IPSG 4G Support

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	IPSG
Applicable Platform(s)	All
Feature Default	Enabled - Always-on (IPSG Licence Required)
Related Changes in This Release	Not Applicable
Related Documentation	*IPSG Administration Guide*

Revision History

Important Revision history details are not provided for features introduced before releases 21.2 and N5.5.

Revision Details	Release
IPSG now supports operating in the 4G RAT environment, which enables IPSG to act as an inline service agent in the core 4G network.	21.3
First introduced.	Pre 21.2

Feature Description

Pre StarOS Release 21.3, IPSG supported only for 3G RAT type. From StarOS Release 21.3, 4G RAT Type and EPS QoS is supported. Support has been extended for IPSG to operate in the 4G RAT environment which enables IPSG to act as an inline service agent in the core 4G network.

Previous Behavior: Earlier, IPSG supported only 3G RAT type and not 4G RAT type.

New Behavior: With StarOS Release 21.3, IPSG supports 4G RAT type. IPSG also supports ULI with TAI+ECGI and TAI, EPS QoS Profile, and generates P-GW CDRs with 4G RAT type.

Customer Impact: 4G calls on IPSG are supported.

EPS QoS Profile Handling

EPS QoS profile handling is done in the following way:

- The QoS profile received from PCRF is given priority as compared to the QoS profile received from the P-GW.
- AMBRs received from PCRF are given priority when there is bandwidth limitation.
- If the Rule Level AMBRs are present, then first, the rule level bandwidth limiting is enforced and then, the APN level AMBR is enforced only for the non-GBR QCI values.
- In the accounting start message, if the QoS profile is received with GBR QCI, then the call is dropped on the IPSG. It is assumed that the QoS profile that is being received on IPSG is of default-bearer on the P-GW.
- If IPSG receives an interim update for a subscriber with a GBR QCI value, then the QCI profile is ignored and no CCR-U is sent to the PCRF.
- If the CLI command **radius accounting interim create-new-call** is configured under the IPSG service and a QoS profile is received with GBR QCI as part of the interim RADIUS update message, then the call is dropped on the IPSG. It is assumed that the QoS profile that is being received on IPSG is of the default bearer on the P-GW.
- To see the QoS profile and QCI information in the CCR-U, you must enable the trigger for the QoS change and default bearer QoS change.

Important As the RAT type is EUTRAN, you must pick the correct P-GW specific dictionary in order to generate the P-GW records.

How It Works

This section lists the working of IPSG:

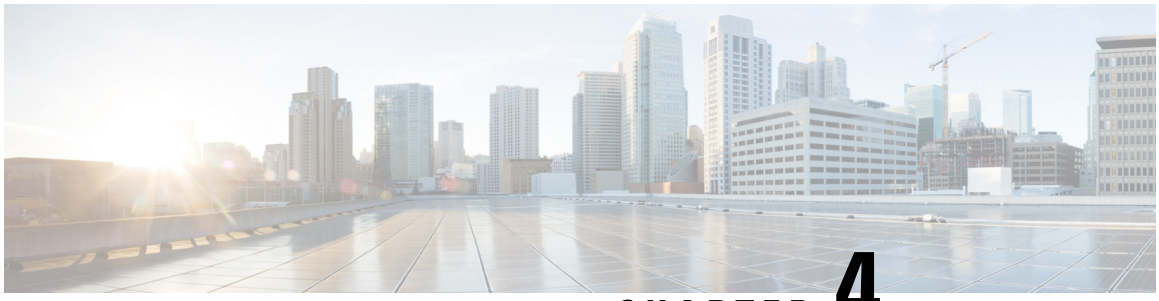
- Support for the EUTRAN RAT type on IPSG creates an EPS bearer.
- The ULI information includes TAI+ECGI, TAI, and ECGI.

- This ULI information is populated to the eGCDRs and the CDRs.
- The EPS QoS information received as part of the RADIUS message is also parsed.
- The bearer type (EPS), RAT Type (eUTRAN, ULI (TAI + ECGI + TAI), and EPS QoS Information that is received as part of RADIUS message is conveyed to the Gx.
- When an interim update is received from the P-GW, IPSG handles this interim update. If the PCRF is registered as ULI change or QoS change, CCR-U is sent to the PCRF with the received information.

Limitations and Restrictions

Following are the limitations of this feature:

- Handoff scenarios are not supported.
- Gy interface is only supported for 4G.
- CoA and disconnect messages handling is not supported.
- IPSG session replacement with EUTRAN is not supported.
- Tethering detection on IPSG is not supported.



CHAPTER 4

Cisco Ultra Traffic Optimization

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• IPSG • P-GW
Applicable Platform(s)	• ASR 5500 • Ultra Gateway Platform
Feature Default	Disabled - License Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *IPSG Administration Guide*

Revision History

Revision Details	Release
With this release, Cisco Ultra Traffic Optimization is qualified on IPSG.	21.8

Overview

In a high-bandwidth bulk data flow scenario, user experience is impacted due to various wireless network conditions and policies like shaping, throttling, and other bottlenecks that induce congestion, especially in the RAN. This results in TCP applying its saw-tooth algorithm for congestion control and impacts user experience, and overall system capacity is not fully utilized.

The Cisco Ultra Traffic Optimization solution provides clientless optimization of TCP and HTTP traffic. This solution is integrated with Cisco P-GW and has the following benefits:

- Increases the capacity of existing cell sites and therefore, enables more traffic transmission.
- Improves Quality of Experience (QoE) of users by providing more bits per second.
- Provides instantaneous stabilizing and maximizing per subscriber throughput, particularly during network congestion.

How Cisco Ultra Traffic Optimization Works

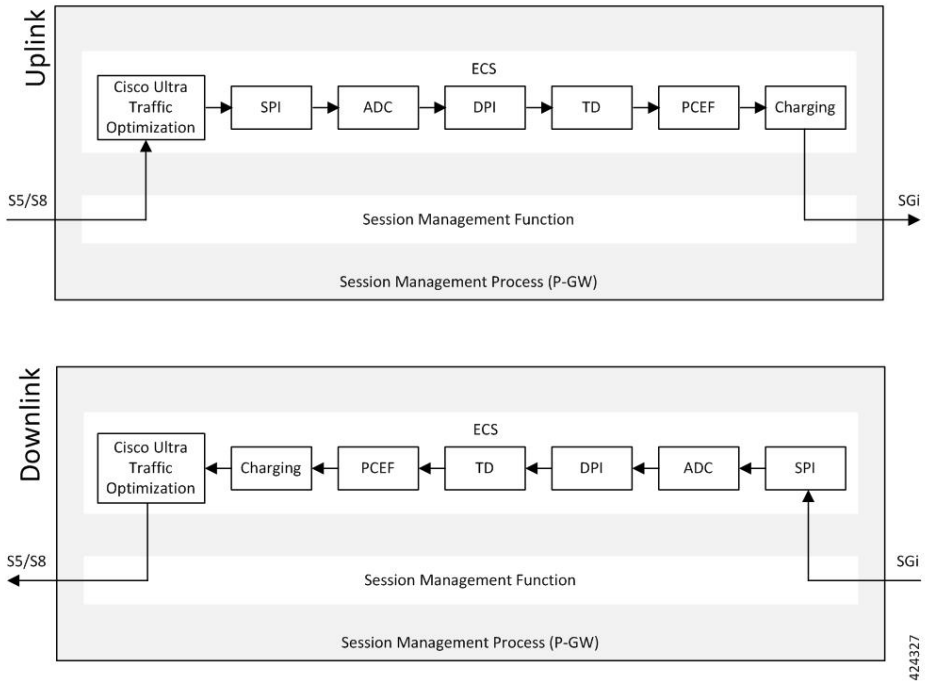
The Cisco Ultra Traffic Optimization achieves its gains by shaping video traffic during times of high network load/congestion. It monitors and profiles each individual video flow that passes through the gateway and uses its machine learning algorithms to determine whether that flow is traversing a congested channel. Cisco Ultra Traffic Optimization then flow-controls video to varying levels and time, depending on the degree of detected congestion, and efficiently aligns delivery of the video traffic to less-congested moments while still providing adequate bandwidth to videos to maintain their quality. The result is less network latency and higher user throughputs while maintaining HD video. Cisco Ultra Traffic Optimization does not drop packets or modify data payloads in any way.

The Cisco Ultra Traffic Optimization integrates with standard Cisco P-GW functions such as Application Detection and Control (ADC), allowing mobile operators to define optimization policies that are based on the traffic application type as well as APN, QCI, and other common traffic delineations. Cisco Ultra Traffic Optimization is fully radio network aware, allowing management on a per eNodeB cell basis.

Architecture

StarOS has a highly optimized packet processing framework, the Cisco Ultra Traffic Optimization engine, where the user packets (downlink) are processed in the operating systems user space. The high-speed packet processing, including the various functions of the P-GW, is performed in the user space. The Cisco Ultra Traffic Optimization engine is integrated into the packet processing path of Cisco's P-GW with a well-defined Application Programming Interface (API) of StarOS.

The following graphic shows a high-level overview of P-GW packet flow with traffic optimization.



Handling of Traffic Optimization Data Record

The Traffic Optimization Data Record (TODR) is generated only on the expiry of idle-timeout of the Cisco Ultra Traffic Optimization engine. No statistics related to session or flow from P-GW is included in this TODR. The data records are a separate file for the Traffic Optimization statistics, and available to external analytics platform.

List of Attributes and File Format

All TODR attributes of traffic optimization is enabled by a single CLI command. The output is always comma separated, and in a rigid format.

Standard TODR

The following is the format of a Standard TODR:

```
instance_id,flow_type,srcIP,dstIP,policy_id, proto_type, dscp,
flow_first_pkt_rx_time_ms,flow_last_pkt_rx_time_ms,flow_cumulative_rx_bytes
```

Example:

```
1,0,173.39.13.38,192.168.3.106,0,1,0,
 1489131332693,1489131335924,342292
```

Where:

- *instance_id*: Instance ID.
- *flow_type*: Standard flow (0)
- *srcIP*: Indicates the source IP address.

- *dstIP*: Indicates the destination IP address.
- *policy_id*: Indicates the traffic optimization policy ID.
- *proto_type*: Indicates the IP protocol being used. The IP protocols are: TCP and UDP.
- *dscp*: Indicates the DSCP code for upstream packets.
- *flow_first_pkt_rx_time_ms*: Indicates the timestamp when the first packet was detected during traffic optimization.
- *flow_last_pkt_rx_time_ms*: Indicates the timestamp when the last packet was detected during traffic optimization.
- *flow_cumulative_rx_bytes*: Indicates the number of bytes transferred by this flow.

Large TODR

The following is a sample output of a Large TODR.

```
19,1,404005123456789,22.22.0.1,1.1.1.8,custom1,2,0,1588858362158,1588858952986,16420806,1588858364162,419,351,7000,0,0,1,
19:2:15,2,0,0,2,1,1,16:0x12546300012345,
1588858364162,80396,1472,0,0,0,2,1,16:0x12546300012345,1588858366171,146942,1937,7000,0,0,2
```

Where:

- *instance_id*: Instance ID.
- *flow_type*: Large flow (1)
- *imsi_id*: Indicates the International Mobile Subscriber Identity.
- *srcIP*: Indicates the source IP address.
- *dstIP*: Indicates the destination IP address.
- *policy_name*: Identifies the name of the configured traffic optimization policy.
- *policy_id*: Indicates the traffic optimization policy ID.
- *proto_type*: Indicates the IP protocol being used. The IP protocols are: TCP and UDP.
- *dscp*: Indicates the DSCP code for upstream packets.
- *flow_first_pkt_rx_time_ms*: Indicates the timestamp when the first packet was detected during traffic optimization.
- *flow_last_pkt_rx_time_ms*: Indicates the timestamp when the last packet was detected during traffic optimization.
- *flow_cumulative_rx_bytes*: Indicates the number of bytes transferred by this flow.
- *large_detection_time_ms*: Indicates the timestamp when the flow was detected as Large.
- *avg_burst_rate_kbps*: Indicates the average rate in Kbps of all the measured bursts.
- *avg_eff_rate_kbps*: Indicates the average effective rate in Kbps.
- *final_link_peak_kbps*: Indicates the highest detected link peak over the life of the Large flow.
- *recovered_capacity_bytes*: Indicates the recovered capacity in Kbps for this Large flow.

- *recovered_capacity_ms*: Indicates the timestamp of recovered capacity for this Large flow.
- *acs_flow_id_count*: Indicates the number of ACS Flow IDs present in this TODR. A maximum of 20 ACS Flow IDs is present.
- *acs_flow_id_list*: Indicates the list of individual ACS Flow IDs. For example, acs_flow_id1, acs_flow_id2, and so on.
- *phase_count*: Indicates the Large flow phase count.
- *min_gbr_kbps*: Indicates the Minimum Guaranteed Bit Rate (GBR) in Kbps.
- *max_gbr_kbps*: Indicates the Maximum Guaranteed Bit Rate (MBR) in Kbps.
- *phase_count_record*: Indicates the number of phases present in this record.
- *end_of_phases*: 0 (not end of phases) or 1 (end of phases).
- Large flow phase attributes:
  - *phase_type*: Indicates the type of the phase. This field represents that the flow was in one of the following three possible states where each state is represented by a numeric value:
    - 0 - Ramp-up Phase (if the Flow was previously idle)
    - 1 - Measurement Phase (required)
    - 2 - Flow Control Phase (if congestion detected during Measurement Phase)
  - *uli_type*: Indicates the type of ULI.
  - *phase_start_time_ms*: Indicates the timestamp for the start time of the phase.
  - *burst_bytes*: Indicates the burst size in bytes.
  - *burst_duration_ms*: Indicates the burst duration in milliseconds.
  - *link_peak_kbps*: Indicates the peak rate for the flow during its life.
  - *flow_control_rate_kbps*: Indicates the rate at which flow control was attempted (or 0 if non-flow control phase). This field is valid only when flow is in 'Flow Control Phase'.
  - *max_num_queued_packets*: Identifies the maximum number of packets queued.
  - *policy_id*: Identifies the traffic optimization policy ID.

Licensing

The Cisco Ultra Traffic Optimization is a licensed Cisco solution. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Limitations and Restrictions

The values which the P-GW chooses to send to the Cisco Ultra Traffic Optimization engine are the values associated from the bearer GBR and bearer MBR. In the current implementation, only downlink GBR and MBR are sent to the engine for traffic optimization.

The IPSG supports only certain triggers for which the information is available with the IPSG service.

Configuring Cisco Ultra Traffic Optimization

This section provides information on enabling support for the Cisco Ultra Traffic Optimization solution.

Loading Traffic Optimization

Use the following configuration under the Global Configuration Mode to load the Cisco Ultra Traffic Optimization as a solution:

```
configure
   require active-charging traffic-optimization
   end
```

Important After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Important Enabling or disabling the traffic optimization can be done through the Service-scheme framework.

Important After you configure the **require active-charging traffic-optimization** CLI command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Important In 21.3, and 21.5 and later releases, the dependency on the chassis reboot is not valid anymore. The Cisco Ultra Traffic Optimization engine is loaded by default. The Cisco Ultra Traffic Optimization configuration CLIs are available when the license is enabled. As such, the **traffic-optimization** keyword has been deprecated.

Enabling Cisco Ultra Traffic Optimization Configuration Profile

Use the following configuration under ACS Configuration Mode to enable the Cisco Ultra Traffic Optimization profile:

```
configure
   active-charging service service_name
      traffic-optimization-profile
      end
```

NOTES:

- The above CLI command enables the Traffic Optimization Profile Configuration, a new configuration mode.

Configuring the Operating Mode

Use the following CLI commands to configure the operating mode under Traffic Optimization Profile Configuration Mode for the Cisco Ultra Traffic Optimization engine:

```
configure
   active-charging service service_name
      traffic-optimization-profile
         mode [ active | passive ]
         end
```

Notes:

- **mode**: Sets the mode of operation for traffic optimization.
- **active**: Active mode where both traffic optimization and flow monitoring is done on the packet.
- **passive**: Passive mode where no flow-control is performed but monitoring is done on the packet.

Configuring Threshold Value

Use the following CLI commands to configure the threshold value for the TCP flow to be considered for the traffic optimization:

```
configure
   active-charging service service_name
      traffic-optimization-profile
         heavy-session detection-threshold bytes
         end
```

Notes:

- **detection-threshold** *bytes*: Specifies the Detection Threshold (in bytes), beyond which it is considered as heavy session.

  bytes must be an integer from 1 to 4294967295.

  For optimum traffic optimization benefits, it is recommended to set the threshold above 3 MB.

Enabling Cisco Ultra Traffic Optimization Configuration Profile Using Service-scheme Framework

The service-scheme framework is used to enable traffic optimization at APN, rule base, QCI, and Rule level. There are two main constructs for the service-scheme framework:

- **Subscriber-base** – This helps in associating subscribers with service-scheme based on the subs-class configuration.
  - **subs-class** – The conditions defined under subs-class enables in classifying the subscribers based on rule base, APN, v-APN name. The conditions can also be defined in combination, and both OR as well as AND operators are supported while evaluating them.
- **Service-scheme** – This helps in associating actions based on trigger conditions which can be triggered either at call-setup time, Bearer-creation time, or flow-creation time.
  - **trigger-condition** – For any trigger, the trigger-action application is based on conditions defined under the trigger-condition.
  - **trigger-actions** – Defines the actions to be taken on the classified flow. These actions can be traffic optimization, throttle-suppress, and so on.

Session Setup Trigger

The **any-match = TRUE**, a wildcard configuration, is the only supported condition for this trigger and so this is applicable to all the flows of the subscriber.

Use the following configuration to setup a Session Trigger:

```
configure
    active-charging service service_name
       trigger-action trigger_action_name
          traffic-optimization
          exit
       trigger-condition trigger_condition_name1
          any-match = TRUE
          exit
       service-scheme service_scheme_name
          trigger sess-setup
             priority priority_value trigger-condition trigger_condition_name1
trigger-action trigger_action_name
             exit
       subs-class sub_class_name
          apn = apn_name
          exit
       subscriber-base subscriber_base_name
          priority priority_value subs-class sub_class_name bind service-scheme
 service_scheme_name
          end
```

Sample Configuration

Following is a sample configuration for Session Setup Trigger:

```
service-scheme SS1
     trigger sess-setup
       priority 1 trigger-condition sess-setup trigger-action sess-setup
     #exit
   trigger-condition sess-setup
     any-match = TRUE
   #exit
   trigger-action sess-setup
     traffic-optimization policy sess-setup
   #exit
```

Bearer Creation Trigger

The trigger conditions related to QCI can be used for this trigger, and so this is applicable to all the flows of specific bearers.

The following is a sample configuration:

```
configure
   active-charging service service_name
      trigger-action trigger_action_name
         traffic-optimization
         exit
      trigger-condition trigger_condition_name1
         any-match = TRUE
         exit
      trigger-condition trigger_condition_name2
         qci = qci_value
         exit
      service-scheme service_scheme_name
         trigger bearer-creation
            priority priority_value trigger-condition trigger_condition_name2
trigger-action trigger_action_name
            exit
         exit
      subs-class sub_class_name
         apn = apn_name
         exit
      subscriber-base subscriber_base_name
         priority priority_value subs-class sub_class_name bind service-scheme
service_scheme_name
         end
```

Flow Creation Trigger

The trigger conditions related to rule-name and QCI can be used here, and so this is related to specific flow.

The following is a sample configuration:

```
configure
   active-charging service service_name
      trigger-action trigger_action_name
         traffic-optimization
         exit
      trigger-condition trigger_condition_name1
         any-match = TRUE
```

```
            exit
        trigger-condition trigger_condition_name2
            qci = qci_value
            exit
        trigger-condition trigger_condition_name3
            rule-name = rule_name
            exit
        service-scheme service_scheme_name
            trigger bearer-creation
               priority priority_value trigger-condition trigger_condition_name3
trigger-action trigger_action_name
               exit
            exit
        subs-class sub_class_name
            apn = apn_name
            exit
        subscriber-base subscriber_base_name
           priority priority_value subs-class sub_class_name bind service-scheme
 service_scheme_name
            end
```

Notes:

- *trigger_condition_name3* can have only rules, only QCI, both rule and QCI, or either of rule and QCI.

The following table illustrates the different levels of Traffic Optimization and their corresponding Subscriber Class configuration and Triggers.

Traffic Optimization Levels	Subscriber Class configuration and Triggers
Applicable to all the calls or flows	**subs-class** *sc1* **any-match = TRUE** **exit** Sessetup trigger condition is **any-match** = **TRUE**
Applicable to all calls or flows of a rulebase	**subs-class** *sc1* **rulebase = prepaid** **exit** Sessetup trigger condition is **any-match** = **TRUE**
Applicable to all calls or flows of an APN	**subs-class** *sc1* **apn = cisco.com** **exit** Sessetup trigger condition is **any-match** = **TRUE**
Applicable to all flows of a Bearer	**trigger-condition** *TC1* **qci = 1** **exit** Bearer creation trigger condition is TC1

Traffic Optimization Levels	Subscriber Class configuration and Triggers
Applicable to a particular flow	**trigger-condition** *TC1* **qci = 1** **rule-name = tcp** **multi-line-or all-lines** **exit** Flow creation trigger condition is TC1

Important In case of LTE to eHRPD handover, since QCI is not valid for eHRPD, it is recommended to configure rule-name as the trigger-condition under service-scheme.

Generating TODR

Use the following CLI commands under ACS Configuration Mode to enable Traffic Optimization Data Record (TODR) generation:

```
configure
   active-charging service service_name
      traffic-optimization-profile
         data-record
         end
```

NOTES:

- If previously configured, use the **no data-record** command to disable generating TODR.

Configuring Rulebase to Allow UDP Traffic Optimization

Important From Release 21.8 onwards, it is recommended to enable TCP and UDP protocol for Traffic Optimization by using the CLI commands mentioned in the *Enabling TCP and UDP* section of this chapter.

Use the following configuration in ACS Rulebase Configuration Mode to turn ON/OFF the traffic optimization for UDP traffic.

Important Enabling/Disabling the Cisco Ultra Traffic Optimization solution is controlled by Service-scheme Framework.

```
configure
  active-charging service service_name
    rulebase rulebase_name
      [ no ] traffic-optimization udp
      end
```

NOTES:

- **udp**: Specifies traffic optimization for UDP traffic.
- By default, UDP traffic optimization is disabled.
- If previously configured, use the **no traffic-optimization udp** CLI command to disable traffic optimization for UDP traffic.

Multi-Policy Support for Traffic Optimization

Cisco Ultra Traffic Optimization engine supports Traffic Optimization for multiple policies and provides Traffic Optimization for a desired location. It supports a maximum of 32 policies that include two pre-configured policies, by default. Operators can configure several parameters under each Traffic Optimization policy.

This feature includes the following functionalities:

- By default, Traffic Optimization is enabled for TCP and UDP data for a particular Subscriber, Bearer, or Flow that use the Service-Schema.

Important PORT 443 supports UDP or QUIC-based Traffic Optimization.

- Selection of a policy depends on the priority configured. A trigger-condition is used to prioritize a traffic optimization policy. The priority is configurable regardless of a specific location where the traffic optimization policy is applied. Based on the configured priorities, a traffic optimization policy can be overridden by another policy.
- A configuration to associate a traffic optimization policy with a Trigger Action, under the Service-Schema.
- A configuration to select a Traffic Optimization policy for a Location Trigger. Currently, only ECGI Change Detection is supported under the Local Policy Service Configuration mode.

Important Location Change Trigger is not supported with IPSG.

Important Policy ID for a flow is not recovered after a Session Recovery (SR) or Inter-Chassis Session Recovery (ICSR).

Important The Multi-Policy Support feature requires the same Cisco Ultra Traffic Optimization license key be installed. Contact your Cisco account representative for detailed information on specific licensing requirements.

How Multi-Policy Support Works

Policy Selection

Cisco's Ultra Traffic Optimization engine provides two default policies – Managed and Unmanaged. When Unmanaged policy is selected, traffic optimization is not performed.

When Managed policy is selected, traffic optimization is performed using default parameters. Managed policy is applied when a policy is not specified in a Trigger Action where traffic optimization is enabled without specifying a policy.

When Managed policy is selected, traffic optimization is performed using default parameters. Managed policy is applied when a policy is not specified in a Trigger Action where traffic optimization is enabled without specifying a policy.

- Session Setup Trigger – If a Trigger Action is applied only for a Session Setup in a Service-Schema, then the trigger action is only applied to new sessions only.
- Bearer Setup Trigger – If a trigger action is applied only for a Bearer Setup, changes in the trigger action will be applicable to newly created bearers and its flows.
- Flow Creation Trigger – Under a trigger condition corresponding to a flow create, conditions can be added based on a rule-name, local-policy-rule or an IP protocol in addition to the trigger condition: any-match.

When traffic optimization on existing flows is disabled because of a trigger condition, then the traffic optimization engine will apply the default Unmanaged policy on them.

Deleting a Policy

Before deleting a Policy profile, all association to a traffic optimization policy should be removed.

For more information on deletion of a policy, refer to the *Traffic Optimization Policy Configuration* section.

Configuring Multi-Policy Support

The following sections describes the required configurations to support the Multi-Policy Support.

Configuring a Traffic Optimization Profile

Use the following CLI commands to configure a Traffic Optimization Profile.

```
configure
  require active-charging
  active-charging service service_name
    traffic-optimization-profile profile_name
      data-record[ large-flows-only | managed-large-flows-only ]
      no data record
      [ no ] efd-flow-cleanup-interval cleanup_interval
      [ no ] stats-interval stats_interval
      [ no ] stats-options { flow-analyst [ flow-trace ] | flow-trace [
 flow-analyst ] }
      end
```

NOTES:

- **require active-charging**: Enables the configuration requirement for an Active Charging service.

  Important After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

- **data-record**: Enables the generation of traffic optimization data record.

  large-flows-only: Enables the traffic optimization data record generation for large flows.

  managed-large-flows-only: Enables the traffic optimization data record generation for managed large flows.

  The keywords - **large-flows-only** and **managed-large-flows-only** when configured along with **data-record** enables the CUTO library to stream the respective statistics as part of the **stats-options** command, to the external server. The operator can configure a combination of the **stats-options** keywords **flow-trace** and **flow-analyst** and the **data-record** command to notify the CUTO library accordingly.

  Note One of the above the two keywords can be configured as part of the data-record, which enables the CUTO library to stream the respective statistics.

  The default behavior of the **data-record** command is not affected with the above implementation . If configured without any of the options, then TODRs are generated for all standard and large flows, which is the existing behavior.

- **efd-flow-cleanup-interval**: Configures the EFD flow cleanup interval. The interval value is an integer that ranges 10–5000 milliseconds.
- **stats-interval**: Configures the flow statistics collection and reporting interval in seconds. The interval value is an integer that ranges 1–60 seconds.
- **stats-options**: Configures options to collect the flow statistics. It only specifies whether the stream must be a Flow Trace or a Flow Analyst or both, to an external server.

Note From Release 21.6 onwards, the **heavy-session** command is deprecated.

Configuring a Traffic Optimization Policy

Use the following CLI commands to configure a Traffic Optimization Policy.

```
configure
  require active-charging
  active-charging service service_name[extended]
    [ no ] traffic-optimization-policy policy_name[extended]
      bandwidth-mgmt { backoff-profile [ managed | unmanaged ] [
```

min-effective-rate *effective_rate* **[min-flow-control-rate** *flow_rate* **] | min-flow-control-rate** *flow_rate* **[min-effective-rate** *effective_rate* **]] | min-effective-rate** *effective_rate* **[backoff-profile [managed | unmanaged] [min-flow-control-rate** *flow_rate* **] | min-flow-control-rate** *control_rate* **[backoff-profile [managed | unmanaged]] | min-flow-control-rate [[backoff-profile [managed | unmanaged] [min-effective-rate** *effective_rate* **] | [min-effective-rate** *effective_rate* **] [backoff-profile [managed | unmanaged]] }**

extended-bandwidth-mgmt { backoff-profile [managed | unmanaged] [min-effective-rate *effective_rate* **[min-flow-control-rate** *flow_rate* **] | min-flow-control-rate** *flow_rate* **[min-effective-rate** *effective_rate* **]] | min-effective-rate** *effective_rate* **[backoff-profile [managed | unmanaged] [min-flow-control-rate** *flow_rate* **] | min-flow-control-rate** *control_rate* **[backoff-profile [managed | unmanaged]] | min-flow-control-rate [[backoff-profile [managed | unmanaged] [min-effective-rate** *effective_rate* **] | [min-effective-rate** *effective_rate* **] [backoff-profile [managed | unmanaged]] }**

[no] bandwidth-mgmt

[no] extended-bandwidth-mgmt

curbing-control { max-phases *max_phase_value* **[rate** *curbing_control_rate* **[threshold-rate** *threshold_rate* **[time** *curbing_control_duration* **]]] | rate** *curbing_control_rate* **[max-phases [threshold-rate** *threshold_rate* **[time** *curbing_control_duration* **]]] | threshold-rate [max-phases** *max_phase_value* **[rate** *curbing_control_rate* **[time** *curbing_control_duration* **]]] | time [max-phases** *max_phase_value* **[rate** *curbing_control_rate* **[threshold-rate** *threshold_rate***]]] }**

extended-curbing-control { max-phases *max_phase_value* **[rate** *curbing_control_rate* **[threshold-rate** *threshold_rate* **[time** *curbing_control_duration* **]]] | rate** *curbing_control_rate* **[max-phases [threshold-rate** *threshold_rate* **[time** *curbing_control_duration* **]]] | threshold-rate [max-phases** *max_phase_value* **[rate** *curbing_control_rate* **[time** *curbing_control_duration* **]]] | time [max-phases** *max_phase_value* **[rate** *curbing_control_rate* **[threshold-rate** *threshold_rate***]]] }**

[no] curbing-control

[no] extended-curbing-control

heavy-session { standard-flow-timeout [threshold *threshold_value* **| threshold** *threshold_value* **[standard-flow-timeout** *timeout_value* **] }**

extended-heavy-session { standard-flow-timeout [threshold *threshold_value* **| threshold** *threshold_value* **[standard-flow-timeout** *timeout_value* **] }**

[no] heavy-session

[no] extended-heavy-session

link-profile { initial-rate *initial_seed_value* **[max-rate** *max_peak_rate_value* **[peak-lock]] | max-rate [initial-rate** *initial_seed_value* **[peak-lock]] | peak-lock [initial-rate** *initial_seed_value* **[max-rate** *max_peak_rate_value* **]] }**

extended-link-profile { initial-rate *initial_seed_value* **[max-rate** *max_peak_rate_value* **[peak-lock]] | max-rate [initial-rate** *initial_seed_value* **[peak-lock]] | peak-lock [initial-rate** *initial_seed_value* **[max-rate** *max_peak_rate_value* **]] }**

[no] link-profile

```
        [ no ] extended-link-profile
        session-params { tcp-ramp-up tcp_rampup_duration [ udp-ramp-up
udp_rampup_duration ] | udp-ramp-up udp_rampup_duration [ tcp-ramp-up
tcp_rampup_duration ] }
       extended-session-params { tcp-ramp-up tcp_rampup_duration [ udp-ramp-up
 udp_rampup_duration ] | udp-ramp-up udp_rampup_duration [ tcp-ramp-up
tcp_rampup_duration ] }
        [ no ] session-params
        [ no ] extended-session-params
        end
```

NOTES:

- Only when **extended** keyword is used after the policy name, you will be able to see the '**extended-***' parameters, for example **extended-bandwidth-mgmt**.
- **no**: Overwrites the configured parameters with default values. The operator must remove all associated policies in a policy profile before deleting a policy profile. Otherwise, the following error message is displayed:

  ```
  Failure: traffic-optimization policy in use, cannot be deleted.
  ```

- **bandwidth-mgmt**: Configures Base bandwidth management parameters.
  - **backoff-profile**: Determines the overall aggressiveness of the back off rates.
  - **managed**: Enables both traffic monitoring and traffic optimization.
  - **unmanaged**: Only enables traffic monitoring.
  - **min-effective-rate**: Configures minimum effective shaping rate in Kbps.
  - **min-flow-control-rate**: Configures the minimum rate that is allowed in Kbps to control the flow of heavy-session-flows during congestion.
- **extended-bandwidth-mgmt**: Configures Extended bandwidth management parameters.
  - **backoff-profile**: Determines the overall aggressiveness of the back off rates.
  - **managed**: Enables both traffic monitoring and traffic optimization.
  - **unmanaged**: Only enables traffic monitoring.
  - **min-effective-rate**: Configures minimum effective shaping rate in Kbps.
  - **min-flow-control-rate**: Configures the minimum rate that is allowed in Kbps to control the flow of heavy-session-flows during congestion.
- **curbing-control**: Configures Base curbing flow control related parameters.
  - **max-phases**: Configures consecutive phases where the target shaping rate is below **threshold-rate** to trigger curbing flow control. .
  - **rate**: Configures the curbing flow-control at a fixed rate in Kbps instead of a dynamic rate.
  - **threshold-rate**: Configures the minimum target shaping rate in kbps to trigger curbing..
  - **time**: Configures the duration of a flow control phase in milliseconds.

- **extended-curbing-control**: Configures Extended curbing flow control related parameters.
  - **max-phases**: Configures consecutive phases where the target shaping rate is below **threshold-rate** to trigger curbing flow control. The maximum phase value is an integer ranging 2–10 for extended parameter. The default value inherits base.
  - **rate**: Configures the curbing flow-control at a fixed rate in Kbps instead of a dynamic rate. The control rate value is an integer ranging 0-100000 kbps for extended parameter. The default value inherits base.
  - **threshold-rate**: Configures the minimum target shaping rate in kbps to trigger curbing.The threshold rate is an integer ranging 100-100000 kbps for extended parameter. The default value inherits base.
  - **time**: Configures the duration of a flow control phase in milliseconds.

    The flow control duration value is an integer ranging 0–600000 for extended parameter. The default value inherits base.

- **heavy-session**: Configures parameters for Base heavy-session detection.
  - **standard-flow-timeout**: Configures the idle timeout in milliseconds, for expiration of standard flows.
  - **threshold**: Configures heavy-session detection threshold in bytes. On reaching the threshold, the flow is monitored and potentially managed..

- **extended-heavy-session**: Configures parameters for Extended heavy-session detection.
  - **standard-flow-timeout**: Configures the idle timeout in milliseconds, for expiration of standard flows. .
  - **threshold**: Configures heavy-session detection threshold in bytes. On reaching the threshold, the flow is monitored and potentially managed.

- **link-profile**: Configures Base link profile parameters.
  - **initial-rate**: Configures the initial seed value of the acquired peak rate in Kbps for a traffic session.
  - **max-rate**: Configures the maximum learned peak rate that is allowed in Kbps for a traffic session.
  - **peak-lock**: Confirms with the link peak rate available at the initial link peak rate setting.

- **extended-link-profile**: Configures Extended link profile parameters.
  - **initial-rate**: Configures the initial seed value of the acquired peak rate in Kbps for a traffic session.
  - **max-rate**: Configures the maximum learned peak rate that is allowed in Kbps for a traffic session.
  - **peak-lock**: Confirms with the link peak rate available at the initial link peak rate setting.

- **session-params**: Configures Base session parameters.
  - **tcp-ramp-up**: Configures the ramp-up-phase duration in milliseconds, for TCP traffic.
  - **udp-ramp-up**: Configures the ramp-up-phase duration in milliseconds, for the UDP traffic..

- **extended-session-params**: Configures Extended session parameters.

- **tcp-ramp-up**: Configures the ramp-up-phase duration in milliseconds, for TCP traffic.
- **udp-ramp-up**: Configures the ramp-up-phase duration in milliseconds, for the UDP traffic..

Important After you configure **require active-charging** command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

The following table shows the parameter ranges for both Base and Extended set parameters, the default values of those parameters and, the validated Range/value for configuring the parameters for Cisco Ultra Traffic Optimization library.

Parameter category (Base/Extended)	Parameter	Base Parameter Range	Base default value	Extended Parameter Range	Extended default value	Range/value check	Comment
bandwidth-mgmt /extended-bandwidth-mgmt	**backoff-profile**	**managed /unmanaged**	**managed**	**managed /unmanaged**	Inherits base	require match base	If you enter a value different from Base, the value from Base parameter and an appropriate message will be displayed.
	min-effective-rate	100-100000 kbps	600	100-500000 kbps	45000	allow full range	
	min-flow-control-rate	100-100000 kbps	250	100- 500000 kbps	1000	allow full range	

Parameter category (Base/Extended)	Parameter	Base Parameter Range	Base default value	Extended Parameter Range	Extended default value	Range/value check	Comment
curbing-control / **extended-curbing-control**	**max-phases**	2-10	2	2-10	Inherits base	allow full range	
	rate	0-100000 kbps	0	0-100000 kbps	Inherits base	allow full range	
	threshold- rate	100-100000 kbps	600	100-100000 kbps	Inherits base	allow full range	
	time	0-600000 ms	0	0-600000 ms	Inherits base	allow full range	
heavy-session / **extended- heavy-session**	**standard-flow-time out**	100-10000 ms	500	100-10000 ms	Inherits base	allow full range	
	threshold	100000–100000000 bytes	3000000	100000–100000000 bytes	Inherits base	allow full range	

Parameter category (Base/Extended)	Parameter	Base Parameter Range	Base default value	Extended Parameter Range	Extended default value	Range/value check	Comment
link-profile / **extended-link-profile**	**initial-rate**	100-100000 kbps	7000	100-500000 kbps	50000	require greater than or equal to base max-rate	If you enter a value different from Base, the value from Base parameter and an appropriate message will be displayed.
	max- rate	100-100000 kbps	15000	100-500000 kbps	100000	require greater than or equal to base max-rate	If you enter a value different from Base, the value from Base parameter and an appropriate message will be displayed.
	peak-lock	enabled/disabled	disabled	enabled/disabled	disabled	allow either	

Parameter category (Base/Extended)	Parameter	Base Parameter Range	Base default value	Extended Parameter Range	Extended default value	Range/value check	Comment
session-params / **extended- session-params**	**tcp-ramp-up**	0-10000 ms	2000	0-10000 ms	2000	allow full range	
	udp-ramp-up	0-10000 ms	2000	0-10000 ms	2000	allow full range	

Traffic Optimization Policy - Default Values

```
Bandwidth-Mgmt:

   Backoff-Profile         : Managed
   Min-Effective-Rate      : 600 (kbps)
   Min-Flow-Control-Rate   : 250 (kbps)

Curbing-Control:

   Time                    : 0 (ms)
   Rate                    : 0 (kbps)
   Max-Phases              : 2
   Threshold-Rate          : 600 (kbps)

Heavy-Session:

   Threshold               : 3000000(bytes)
   Standard-Flow-Timeout   : 500 (ms)

Link-Profile:

   Initial-Rate            : 7000 (kbps)
   Max-Rate                : 15000 (kbps)
   Peak-Lock               : Disabled

Session-Params:

   Tcp-Ramp-Up             : 2000 (ms)
   Udp-Ramp-Up             : 2000 (ms)
```

Associating a Trigger Action to a Traffic Optimization Policy

Use the following CLI commands to associate a Trigger Action to a Traffic Optimization Policy.

```
configure
   require active-charging
   active-charging service service_name
      trigger-action trigger_action_name
         traffic-optimization policy policy_name
         [ no ] traffic-optimization
         end
```

NOTES:

- **traffic-optimization policy**: Configures a traffic optimization policy.
- **no**: Removes the configured traffic optimization policy.

Enabling TCP and UDP

Use the following CLI commands to enable TCP and UDP protocol for Traffic Optimization:

```
configure
   require active-charging
   active-charging service service_name
      trigger-condition trigger_condition_name
         [ no ] ip protocol = [ tcp | udp ]
         end
```

NOTES:

- **no**: Deletes the Active Charging Service related configuration.
- **ip**: Establishes an IP configuration.
- **protocol**: Indicates the protocol being transported by the IP packet.
- **tcp**: Indicates the TCP protocol to be transported by the IP packet.
- **udp**: Indicates the UDP protocol to be transported by the IP packet.

Important After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Service-Scheme Configuration for Multi-Policy Support

The service-schema framework enables traffic optimization at APN, rule base, QCI, and Rule level. With the Multi-Policy Support feature, traffic optimization in a service-scheme framework allows the operator to configure multiple policies and to configure traffic optimization based on a desirable location.

The service-scheme framework helps in associating actions based on trigger conditions, which can be triggered either at call-setup time, Bearer-creation time, or flow-creation time.

Monitoring and Troubleshooting

This section provides information regarding commands available to monitor and troubleshoot the Cisco Ultra Traffic Optimization solution on the P-GW.

Cisco Ultra Traffic Optimization Show Commands and/or Outputs

This section provides information about show commands and the fields that are introduced in support of Cisco Ultra Traffic Optimization solution.

show active-charging rulebase name <rulebase_name>

The output of this show command has been enhanced to display if the UDP traffic optimization is Enabled or Disabled. Following are the fields that has been introduced:

- Traffic Optimization:
  - UDP: Enabled/Disabled

show active-charging traffic-optimization counters

The **show active-charging traffic-optimization counters sessmgr { all | instance** *number* **}** CLI command is introduced where:

- **counters** – Displays aggregate flow counters/statistics from Cisco Ultra Traffic Optimization engine.

Important This CLI command is license dependent and visible only if the license is loaded.

Following are the new field/counters:

- Traffic Optimization Flows:
  - Active Normal Flow Count
  - Active Large Flow Count
  - Active Managed Large Flow Count
  - Active Unmanaged Large Flow Count
  - Base Policy:
    - Active Large Flow Count
    - Active Managed Large Flow Count
    - Active Unmanaged Large Flow Count
  - Extended Policy:
    - Active Large Flow Count
    - Active Managed Large Flow Count
    - Active Unmanaged Large Flow Count
  - Total Normal Flow Count
  - Total Large Flow Count
  - Total Managed Large Flow Count
  - Total Unmanaged Large Flow Count
  - Base Policy:
    - Total Large Flow Count
    - Total Managed Large Flow Count
    - Total Unmanaged Large Flow Count

- Extended Policy:
  - Total Large Flow Count
  - Total Managed Large Flow Count
  - Total Unmanaged Large Flow Count
- Total IO Bytes
- Total Large Flow Bytes
- Total Recovered Capacity Bytes
- Total Recovered Capacity ms

On executing the above command, the following new fields are displayed for the Multi-Policy Support feature:

Important This CLI command is license dependent and visible only if the license is loaded.

- TCP Traffic Optimization Flows:
  - Active Normal Flow Count
  - Active Large Flow Count
  - Active Managed Large Flow Count
  - Active Unmanaged Large Flow Count
  - Base Policy:
    - Active Large Flow Count
    - Active Managed Large Flow Count
    - Active Unmanaged Large Flow Count
  - Extended Policy:
    - Active Large Flow Count
    - Active Managed Large Flow Count
    - Active Unmanaged Large Flow Count
  - Total Normal Flow Count
  - Total Large Flow Count
  - Total Managed Large Flow Count
  - Total Unmanaged Large Flow Count
  - Base Policy:
    - Total Large Flow Count

        - Total Managed Large Flow Count
        - Total Unmanaged Large Flow Count
    - Extended Policy:
        - Total Large Flow Count
        - Total Managed Large Flow Count
        - Total Unmanaged Large Flow Count
    - Total IO Bytes
    - Total Large Flow Bytes
    - Total Recovered Capacity Bytes
    - Total Recovered Capacity ms
- UDP Traffic Optimization Flows:
    - Active Normal Flow Count
    - Active Large Flow Count
    - Active Managed Large Flow Count
    - Active Unmanaged Large Flow Count
    - Base Policy:
        - Active Large Flow Count
        - Active Managed Large Flow Count
        - Active Unmanaged Large Flow Count
    - Extended Policy:
        - Active Large Flow Count
        - Active Managed Large Flow Count
        - Active Unmanaged Large Flow Count
-
    - Total Normal Flow Count
    - Total Large Flow Count
    - Total Managed Large Flow Count
    - Total Unmanaged Large Flow Count
    - Base Policy:
        - Total Large Flow Count
        - Total Managed Large Flow Count

- Total Unmanaged Large Flow Count

- Extended Policy:
  - Total Large Flow Count
  - Total Managed Large Flow Count
  - Total Unmanaged Large Flow Count

- Total IO Bytes:
- Total Large Flow Bytes
- Total Recovered Capacity Bytes
- Total Recovered Capacity ms

show active-charging traffic-optimization info

This show command has been introduced in Exec Mode, where:

- **traffic-optimization** – Displays all traffic optimization options.
- **info** – Displays Cisco Ultra Traffic Optimization engine information.

The output of this CLI command displays the version, mode, and configuration values.

Following are the new fields/counters:

- Version:
- Mode:
- Configuration:
  - Data Records (TODR)
  - Statistics Options
  - EFD Flow Cleanup Interval
  - Statistics Interval

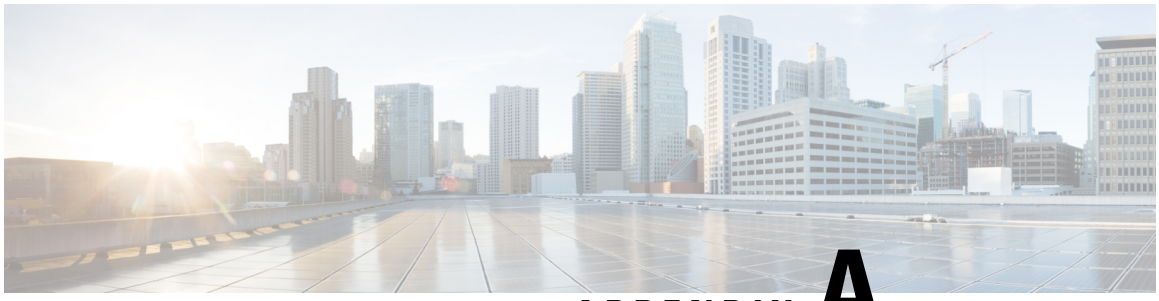
show active-charging traffic-optimization policy

On executing the above command, the following new fields are displayed for the Multi-Policy Support feature:

- Policy Name
- Policy-Id
- Bandwidth-Mgmt
  - Backoff-Profile
  - Min-Effective-Rate

    - Min-Flow-Control-Rate
- Extended-Bandwidth-Mgmt
    - Backoff-Profile
    - Min-Effective-Rate
    - Min-Flow-Control-Rate
- Curbing-Control
    - Time
    - Rate
    - Max-phases
    - Threshold-Rate
- Extended-Curbing-Control
    - Time
    - Rate
    - Max-phases
    - Threshold-Rate
- Heavy-Session
    - Threshold
    - Standard-Flow-Timeout
- Extended-Heavy-Session
    - Threshold
    - Standard-Flow-Timeout
- Link-Profile
    - Initial-Rate
    - Max-Rate
    - Peak-Lock
- Extended-Link-Profile
    - Initial-Rate
    - Max-Rate
    - Peak-Lock
- Session-Params

    - Tcp-Ramp-Up
    - Udp-Ramp-Up
- Extended-Session-Params
    - Tcp-Ramp-Up
    - Udp-Ramp-Up



APPENDIX A

IP Services Gateway AAA AVP Support

This appendix presents a quick reference for message-level AVP support for the IPSG.

The following table describes the indicators used in the quick reference table.

Table 3: Indicators used in the Quick Reference Table

Indicator	Description
M	Mandatory, one or more instances of the AVP MUST be present in the message.
O	Optional, zero or more instances of the AVP MAY be present in the message.
C	Conditional, the AVP can be mandatory or optional depending on the dictionary used.

Table 4: IPSG AVP Support Quick Reference Table

Attribute	Accounting-Request-Start	Accounting-Request-Interim	Accounting-Request-Stop	Access-Request	Disconnect-Message Request (PoD message initiated by IPSG)	Notes
User-Name	C	C	C	C	C	Optional for custom54. If this AVP is present, it is used. Else a default value "void" will be used as username in ipsgmgr. Mandatory for starent-vsa1.
Acct-Status-Type	M	M	M	M	M	
Acct-Session-Id	M	M	M	O	M	

IP Services Gateway AAA AVP Support

Attribute	Accounting-Request-Start	Accounting-Request-Interim	Accounting-Request-Stop	Access-Request	Disconnect-Message Request (PoD message initiated by IPSG)	Notes
Framed-IP-Address	M	M	M	O	M	Mandatory if Framed-Ipv6-Prefix in not present
Framed-Ipv6-Prefix	M	M	M	O	M	Mandatory if Framed-IP-Address is not present
Calling-Station-ID	C	C	C	C	C	Optional for starent-vsa1. Even though the AVP is present, it will be set to NULL and processed by ipsgmgr. Mandatory for custom54.
Called-Station-ID	M	M	M	M	O	Optional for profile subscriber
User-Password	O	O	O	O	O	
Event-Timestamp	O	O	O	O	O	
NAS-Port-Id	O	O	O	O	O	
NAS-Port	O	O	O	O	O	
NAS-Port-Type	O	O	O	O	O	
NAS-IP-Address	O	O	O	O	O	IPv4 address of the GGSN for communication with the AAA server.
NAS-Identifier	O	O	O	O	O	Hostname of the GGSN for communication with the AAA server.
Framed-Protocol	O	O	O	O	O	
Acct-Input-Packets	O	O	O	O	O	

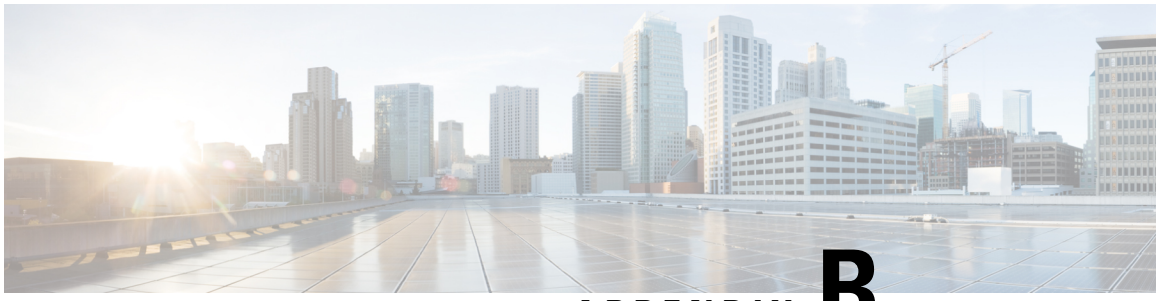
Attribute	Accounting-Request-Start	Accounting-Request-Interim	Accounting-Request-Stop	Access-Request	Disconnect-Message Request (PoD message initiated by IPSG)	Notes
Acct-Output-Packets	O	O	O	O	O	
Acct-Authentic	O	O	O	O	O	
Acct-Delay-Time	O	O	O	O	O	
Vendor-Specific	O	O	O	O	O	
Class	O	O	O	O	O	
Service-Type	O	O	O	O	O	
Connect-Info	O	O	O	O	O	
Proxy-State	O	O	O	O	O	
3GPP-IMSI	O	O	O	O	O	Optional, otherwise IPSG configured value used in CPC Request.
3GPP-Charging Characteristics	O	O	O	O	O	Contains the charging characteristics for this PDP context received in the Create PDP Context request message.
3GPP-Negotiated-QoS-Profile	O	O	O	O	O	Represents the QoS profile for the PDP context.
3GPP-GGSN-MCC-MNC	O	O	O	O	O	MCC-MNC of the network the GGSN belongs to.

IP Services Gateway AAA AVP Support

Attribute	Accounting-Request-Start	Accounting-Request-Interim	Accounting-Request-Stop	Access-Request	Disconnect-Message Request (PoD message initiated by IPSG)	Notes
3GPP-SGSN-MCC-MNC	O	O	O	O	O	For GGSN and PGW connected to a Gn/Gp SGSN, it represents the MCC and MNC extracted from the RAI within the Create PDP Context Request or Update PDP ContextRequest message. For P-GW in GTP/PMIP S5/S8 it represents the MCC and MNC extracted from the Serving Network.
3GPP-RAT-Type	O	O	O	O	O	
3GPP-SGSN-Address	O	O	O	O	O	
3GPP-GGSN-Address	O	O	O	O	O	It represents the IPv4 address that is used by the GTP control plane for the context establishment.
3GPP-User-Location-Info	O	O	O	O	O	Used to inform the change in user location.
3GPP-IMEISV	O	O	O	O	O	
3GPP-Charging-Id	O	O	O	O	O	

Attribute	Accounting-Request-Start	Accounting-Request-Interim	Accounting-Request-Stop	Access-Request	Disconnect-Message Request (PoD message initiated by IPSG)	Notes
3GPP-Selection-Mode	O	O	O	O	O	Not used in IPSG.Contains the selection mode for this PDP context received in the Create PDP Context request message.
3GPP-NSAPI	O	O	O	O	O	Identifies a particular PDP context for the associated PDN and MSISDN/IMSI from creation to deletion.
3GPP-PDP-Type	O	O	O	O	O	Not used in IPSG. PDP type determined based on IPv4 or IPv6 address.
3GPP-MS-TimeZone	O	O	O	O	O	
SN-Transparent-Data	O	O	O	O	O	
SN1-Transparent-Data	O	O	O	O	O	
SN-Assigned-VLAN-ID	O	O	O	O	O	
SN1-Assigned-VLAN-ID	O	O	O	O	O	
SN1-Vpn-Name	C	C	C	C	C	Mandatory if the Overlapping IP Address feature is enabled.

IP Services Gateway AAA AVP Support



APPENDIX B

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.

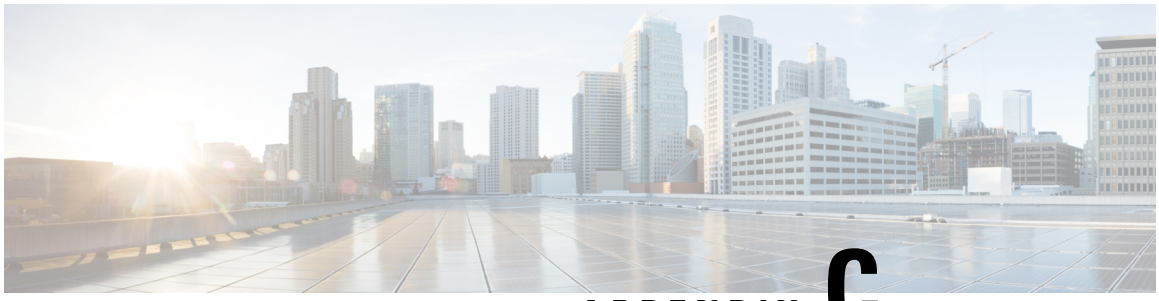
The following rules are covered in this appendix:

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.
- Regardless of number of contexts in the configuration, **ingress-mode** CLI command must be configured for ASR5500 and VPC-SI or VPC-DI platforms. This is done to give precedence to the two matching flows. For example, cases when IPv4SA or IPv4DA both are matched for the ingress packet, then if the incoming interface is designated as ingress, the lookup will be performed in the order of IPv4SA first and then IPv4DA. But if the ingress mode is not set, priority is given to the IPv4DA flow. This is true only for ASR5500 and later platforms such as VPC-SI and VPC-DI.

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.



APPENDIX C

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 functions, commands, and keywords/variables are available or supported for all network function or services. This depends on the platform type and the installed license(s).

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 *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.

License Requirements

The RADIUS Change of Authorization (CoA) and Disconnect Message (DM) are licensed Cisco features. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

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 Enabling CoA and DM, on page 64.

Step 2 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Step 3 View CoA and DM message statistics as described in Viewing CoA and DM Statistics, on page 67.

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. 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.

  For more information on configuring the AAA context, if you are using StarOS 12.3 or an earlier release, refer to the *Configuring Context-Level AAA Functionality* section of the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *AAA 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 *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)

Important Functionality described for this feature in this segment is not applicable for HNB-GW sessions.

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.

License Requirements

The Session Redirection (Hotlining) is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

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 *System Administration Guide*. For more information on **readdress server**, refer to the *ACL Configuration Mode Commands* chapter of the *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 RADIUS Change of Authorization and Disconnect Message, on page 63.

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:

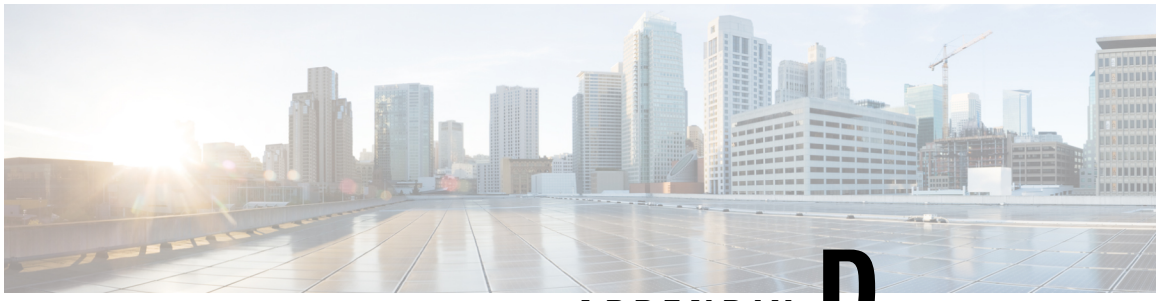
```
username: user1 callid: 01ca11b1    msid: 0000100003
  Card/Cpu: 4/2
  Sessmgr Instance: 7
  Primary callline:
  Redundancy Status: Original Session
  Checkpoints   Attempts    Success    Last-Attempt   Last-Success
     Full:            27         26         15700ms        15700ms
     Micro:           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
```

CoA, RADIUS DM, and Session Redirection (Hotlining)

```
            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
```

CoA, RADIUS DM, and Session Redirection (Hotlining)

```
       Failure (other reasons):  0
Redirected Session Entries:
       Allowed:                  2000      Current:                  0
       Added:                    0         Deleted:                  0
       Revoked for use by different subscriber: 0
```



APPENDIX D

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. 7 Gx Interface

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

- GGSN
- IPSG

This section describes the following topics:

Introduction

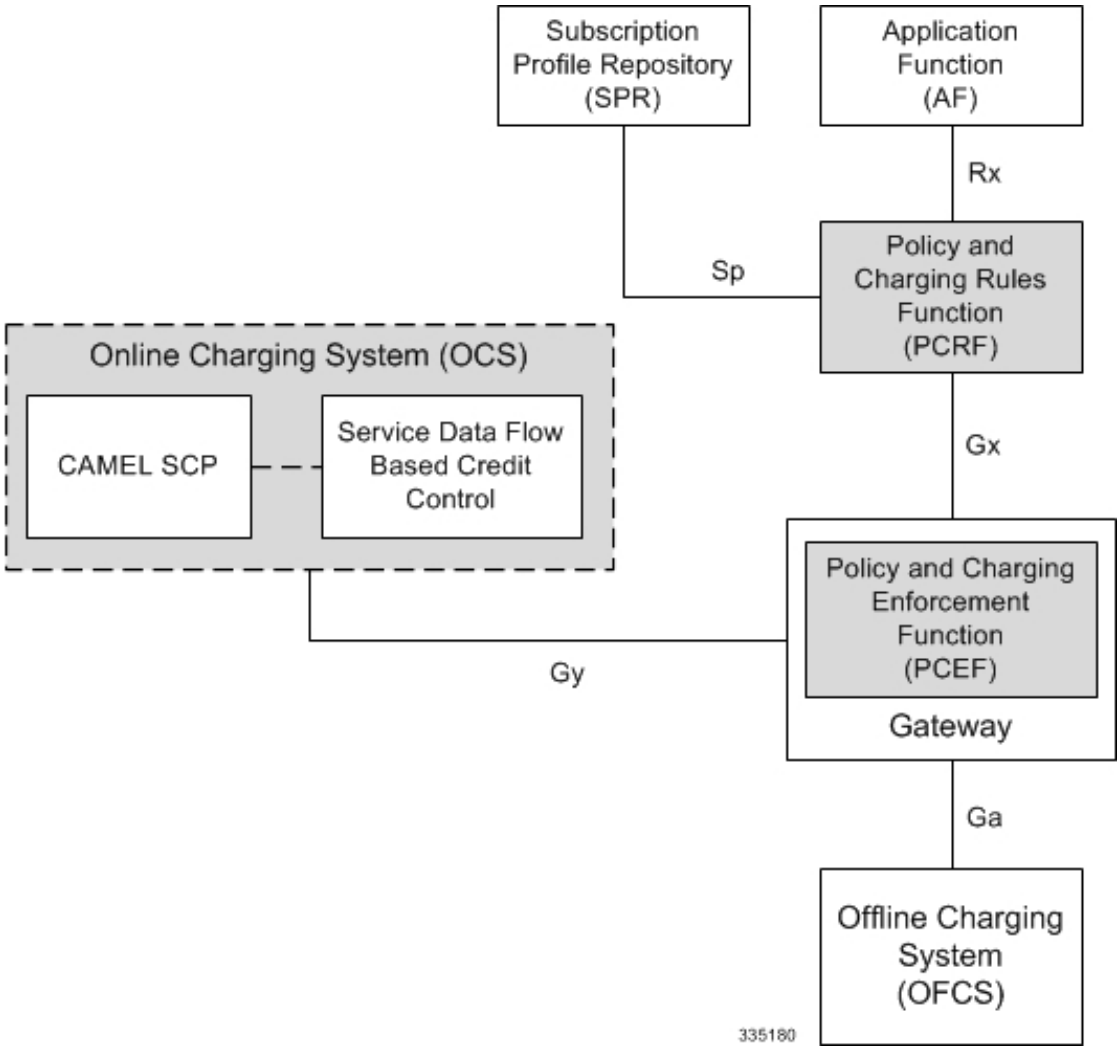
For IMS deployment in GPRS/UMTS networks the system uses Rel. 7 Gx interface for policy-based admission control support and flow-based charging. The Rel. 7 Gx interface supports enforcing policy control features like gating, bandwidth limiting, and so on, and also supports flow-based charging. This is 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.

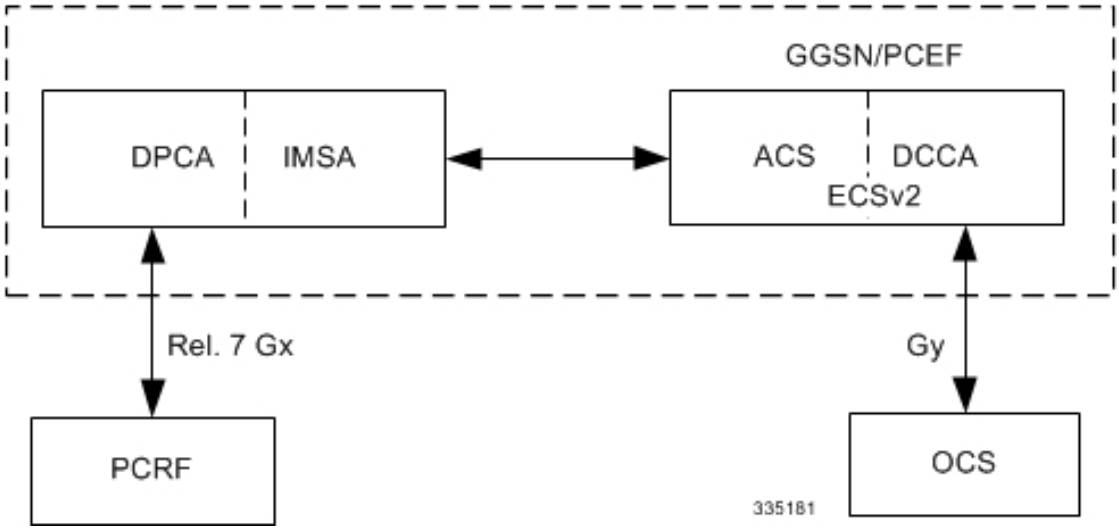
The Rel. 7 Gx reference point is located between the Gateway and the PCRF. This reference point is used for provisioning and removal of PCC rules from the PCRF to the Gateway, and the transmission of traffic plane events from the Gateway to the PCRF. The Gx reference point can be used for charging control, 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 chassis with StarOS Release 8.1 and later running GGSN service for the core network services.

License Requirements

The Rel. 7 Gx interface support is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *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.

  Prior to Release 16.0, the rule binding was getting rejected. In 16.0 and later releases, the binding of PCEF rules will be successful when BCM mode is set to UE-only for EPS IP-CAN bearer without "bearer-ID" in the PCRF messages such as RAR or CCA-U.

  In the 3G to 4G handover scenario, rule binding and rule removal will be successful in UE-only mode and any filter (and related info) changes because of this modification/installation/removal will not be notified to UE as updates in UE only mode cannot be sent to UE. These rules are only considered for charging and the expectation is that the same rules are again modified in 4G (if handover is done) so that the filters (and related info) can be notified to UE.

  In releases prior to 18, P-GW/GGSN does not send CCR-U with Charging Rule report for rule binding failure occurred during 4G to 3G HO in a collision case where create/update bearer response in 3G/4G is pending and update bearer of 3G HO is received. In 18 and later releases, CCR-U is generated and sent to PCRF for reporting rule failure when the collision happens during GnGp HO scenario.

  This additional Gx message (CCR-U) triggered will require multiple CCR-Us to be configured when RAT_TYPE trigger is enabled. Otherwise, the subscriber call will be dropped whenever the collision happens during HO.

- **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.

Gx Interface Support

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.

  In StarOS releases prior to 14.0, SUCCESSFUL_RESOURCE_ALLOCATION (22) event trigger was sent for rules irrespective of successful installation. In 14.0 and later releases, SUCCESSFUL_RESOURCE_ALLOCATION (22) event trigger will be sent under the following conditions:

  - When a rule is installed successfully (and the event trigger is armed by PCRF and resource-allocation-notification is enabled).
  - On partial failure, i.e., when two or more rules are installed and at least one of the rules were successfully installed. (and the event trigger is armed by PCRF and resource-allocation-notification is enabled).

  On complete failure, i.e., none of the rules were installed, the event-trigger SUCCESSFUL_RESOURCE_ALLOCATION (22) will not be sent.

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.

    Important Only standards-based QCI values of 1 through 9 are supported. QCI values 1 through 9 are defined in 3GPP Specification TS 23.203 "Policy and charging control architecture".

  - 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 sends the PCRF a new CCR command and include a 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 releases prior to 18, P-GW/GGSN does not send CCR-U with Charging Rule report for rule binding failure occurred during 4G to 3G HO in a collision case where create/update bearer response in 3G/4G is pending and update bearer of 3G HO is received. In 18 and later releases, CCR-U is generated and sent to PCRF for reporting rule failure when the collision happens during GnGp HO scenario.

This additional Gx message (CCR-U) triggered will require multiple CCR-Us to be configured when RAT_TYPE trigger is enabled. Otherwise, the subscriber call will be dropped whenever the collision happens during HO.

- 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.

In releases prior to 17.0, if "Rule-Deactivation-Time" AVP for a predefined rule was omitted in a CCA-U or RAR message, then any previous value for this AVP was continued to be used in the chassis. In 17.0 and later releases, if Rule-Deactivation-Time AVP is omitted in CCA/RAR, then any previous value for this AVP is no longer valid. The new behavior is compliant to the 3GPP specification for Gx, version 12.1.0.

If PCRF enables the same predefined rule again in RAR/CCA-U without Rule-Deactivation-Time AVP, then the deactivation-time for this rule, if any, will be removed.

For switching to the old behavior, PCRF should re-send the same value of Rule-Deactivation-Time AVP along with predef-rule name in the PCRF message (RAR, CCA-U).

Important This behavior change is applicable only to predefined rules.

Support for Firewall Policy on Gx: The Diameter AVP "SN-Firewall-Policy" has been added to the Diameter dynamic dictionary to support Firewall policy on Gx interface. This AVP can be encoded in CCA-I message to apply/overwrite the fw-and-nat policy that has either been statically assigned to the PDP context via APN configuration or dynamically assigned via RADIUS in Access-Accept. This AVP can also parsed in any CCA-U or RAR message to modify the fw-and-nat policy that is currently assigned to the PDP context.

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 or the peer names).

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. The Online/Offline AVP received at command level applies only to dynamic rules if they are not configured at PCC rule level.

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 installed, modified, and removed 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.

Important ASR 5500 supports only eight flow information including the flow description per dynamic charging rule in a Gx message.

In releases prior to 14.0, there were only 10 PCC rules that were recovered per bearer in the event of a session manager crash. In 14.0 and later releases, this limit has been increased to 24. That is, up to 24 PCC rules can be recovered post ICSR.

With the increase in the limit of PCC rules that can be recovered, the rules are not lost and hence the charging applied to the end users are not impacted.

In releases prior to 17.0, when P-GW received PCC rules from PCRF and it results in Create Bearer or Update Bearer to be triggered towards MME/S-GW, the PCC rules were kept in a pending-active state. Any modification request that was received for these pending-active rules were not currently honored by the P-GW. In 17.0 and later releases, when modification for the PCC rules in pending-active state is received, the modified parameters will be buffered at P-GW. After the response for the pending request is received from the access network, P-GW will process the modification of the buffered parameters and if required generate another update towards network.

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.

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.

Releases prior to 14.0, when PCRF has subscribed to Out of Credit trigger, on session connect when one rule validation fails and also when an Out of Credit was received from OCS for another rule, P-GW was trying to report these failures in different CCR-U to PCRF. However, the second CCR-U of Out of credit was getting dropped internally.

In 14.0 and later releases, on session connect, P-GW combines the rule failure and out of credit in the same CCR-U and sends to PCRF.

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 Requirements

The Volume Reporting over Gx is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Important In 12.0 and later releases, no separate license is required for Charging over Gx / Volume Reporting over Gx feature. This feature can be enabled as part of "Policy Interface" license.

Supported Standards

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

3GPP TS 29.212 V9.5.0 (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.

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.

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

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.

In 12.2 and later releases, usage reporting on bearer termination is supported.

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.

Gx Interface Support

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.

In releases prior to 17.0, extra CCR-U was generated for a monitoring key when the following requests are received in the response to the CCR-U which reported the usage for the same monitoring key.

- immediate reporting request with monitoring key at rule level
- immediate reporting request with or without monitoring key at session level
- explicit disable request at rule level
- explicit disable request at session level

In 17.0 and later releases, extra CCR-U is not generated for a monitoring key when all the above mentioned requests are received in the response to the CCR-U which reported the usage for the same monitoring key. Also, extra CCR-U is not generated when immediate reporting request without monitoring key at rule level is received in the response to the CCR-U which reported the usage for all the active monitoring keys.

- 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 the 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.

In releases prior to 15.0, when threshold breach happens for multiple monitoring keys at the same time, only one of the monitoring keys' usage is reported and the rest of the monitoring keys' usage is reported in CCR-T (threshold set to infinity). On Tx expiry/TCP link error, unreported usage is stored at ECS and reported only on session termination.

In 15.0 and later releases, only one of the monitoring keys' usage is reported first. Upon receiving successful response from PCRF, the rest of the monitoring keys' usage is reported to PCRF. On Tx expiry/TCP link error, unreported usage is stored at ECS. Any future successful interaction with PCRF for the session will send unreported UMI to PCRF.

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.

  PCRF uses RAR message and includes Session-Release-Cause AVP in it to initiate IP CAN Session Termination. However, there are some scenarios where PCRF may want to terminate the IP CAN Session in CCA messages. In order to avoid an unnecessary additional message, PCRF can inform P-GW to terminate the subscriber in CCA-U message itself. Hence, in 17.0 and later releases, the Session Release Cause has been added in CCA messages for all Gx dictionaries.

- 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.

Releases prior to 14.0, when PCC rule was tried to be removed while waiting for access side update bearer response, the charging rules were not removed. In 14.0 and later releases, on receiving message from PCRF, the rule that is meant for removal is marked and then after the access side procedure is complete the rule is removed.

- 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.
- Release 12.2 onwards, usage reporting on bearer termination can be added. When a bearer is deleted due to some reason, the rules associated with the bearer will also be removed. So, the usage will be reported on the monitoring key(s) whose associated rule is the last one that is removed because of bearer termination.
- 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.

In releases prior to 17.0, CCR-U triggered on server retries does not take server granted quota into account for reporting USU. In 17.0 and later releases, CCR-U triggered on server retries takes server granted quota into account for reporting USU. For newly created MSCC, interim quota configuration is taken as reference for reporting USU.

For information on how to configure the Volume Reporting over Gx feature, see Configuring Volume Reporting over Gx, on page 99.

ICSR Support for Volume Reporting over Gx (VoRoGx)

In releases prior to 15.0, post the ICSR switchover, any existing session for which the PCRF has enabled volume reporting used to continue indefinitely until the session is terminated or until CCR-U is sent for a given trigger, without having the volume counted via Gx.

To summarize, after an ICSR switchover, volume reporting over Gx is no longer done for existing sessions. Also, volume usage is not synced to standby chassis.

In 15.0 and later releases, volume threshold and volume usage are synced to standby chassis to support volume reporting over Gx for existing sessions post switchover.

Without this support it cannot cause a subscriber to use higher speeds than what s/he is supposed to get, if volume reporting is for example used to enforce fair usage; the operator may already consider this a revenue loss. It will also severely impact roaming subscribers who are supposed to get a notification and be blocked/redirected once the limits set by the EU roaming regulation are reached. If a session continues now without being blocked, the operator is not allowed to charge for data beyond the limit and will have a significant and real revenue loss (roaming partner may still charge for the data used on their SGSNs).

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.

Important In 14.0 and later releases, the DPCA and the IMSA will be acting as one module within the Policy Server interface application.

Gx Interface Support

Figure 10: Rel. 7 Gx IMS Authorization Call Flow

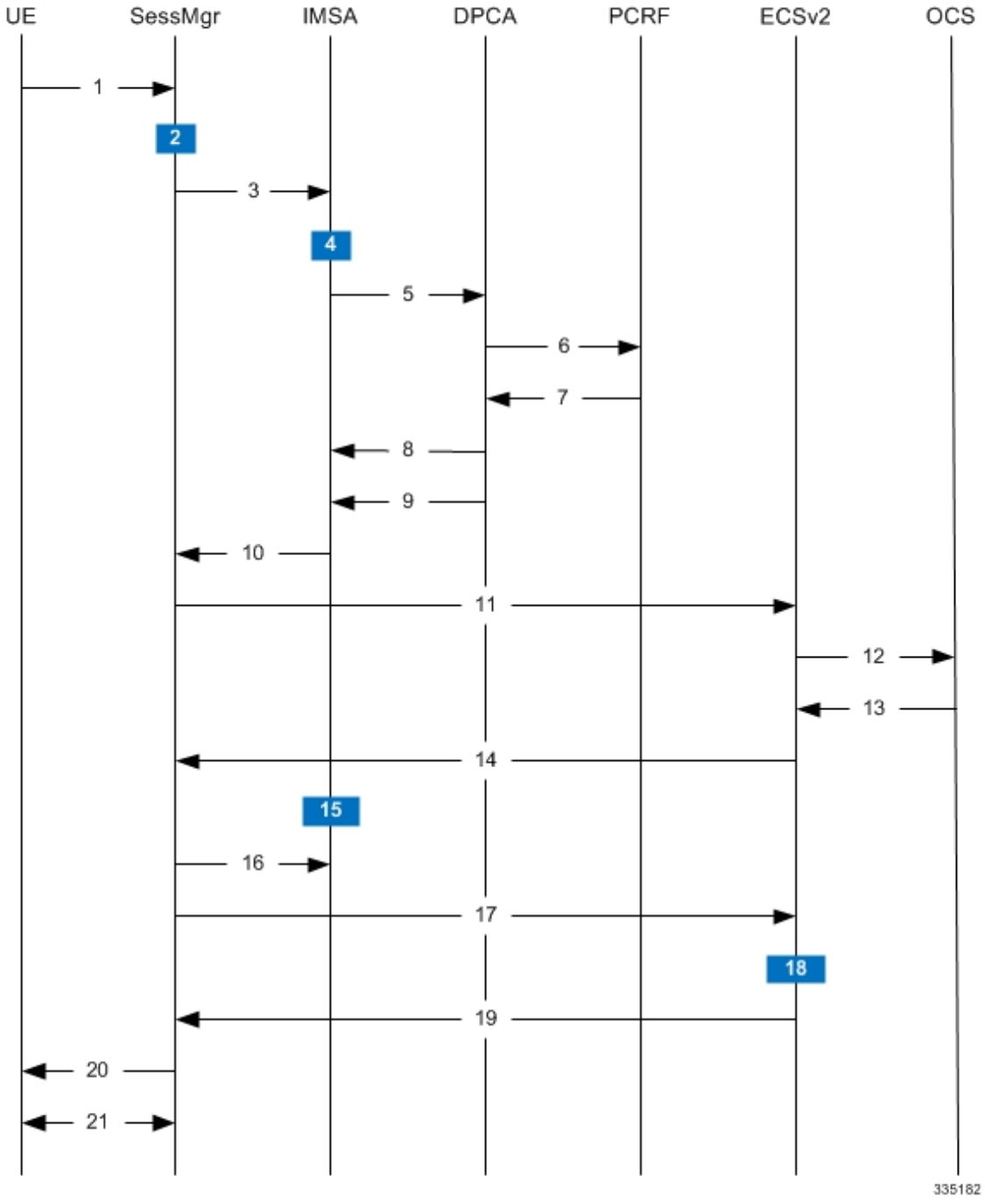


Table 5: Rel. 7 Gx IMS Authorization Call flow Description

Step	Description
1	UE (IMS subscriber) requests for primary PDP context activation/creation.

Step	Description
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.
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.

Gx Interface Support

Step	Description
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, in 14.0 and later releases, the RAR messages are allowed before the session is established. In earlier releases, until the primary PDP context is established, all RAR messages from the PCRF were rejected. Also note that, in 14.0 and later releases, the RAR message is rejected and RAA is sent with 3002 result code when the recovery of dynamic rule information and audit of Session Manager are in progress. Earlier, the RAR messages were processed by DPCA even when the recovery audit was in progress.
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.

Step	Description
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 Configuring IMS Authorization Service at Context Level, on page 96.

Step 2 Verify your configuration as described in Verifying the Configuration, on page 98.

Step 3 Configure an APN within the same context to use the IMS Authorization service for IMS subscriber as described in Applying IMS Authorization Service to an APN, on page 98.

Step 4 Verify your configuration as described in Verifying Subscriber Configuration, on page 99.

Step 5 *Optional:* Configure the Volume Reporting over Gx feature as described in Configuring Volume Reporting over Gx, on page 99.

Step 6 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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.

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.
- In releases prior to 18, a maximum of 16 authorization services can be configured globally in the system. There is also a system limit for the maximum number of total configured services. In 18 and later releases, up to a maximum of 30 IMS authorization service profiles can be configured within the system.
- Secondary P-CSCF IP address can be configured in the P-CSCF table. Refer to the *Command Line Interface Reference* for more information on the **p-cscf table** command.

  In 18 and later releases, the syntax for **p-cscf table** configuration command is:

  ```
  p-cscf table { 1 | 2 } row-precedence precedence_value { ipv4-address
  ipv4_address [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [
  ipv4-address ipv4_address ] } [ secondary { ipv4-address ipv4_address [
  ```

ipv6-address *ipv6_address* **]** **|** **ipv6-address** *ipv6_address* **[** **ipv4-address** *ipv4_address* **]** **}** **[** **weight** *value* **]**

- To enable Rel. 7 Gx interface support, pertinent Diameter dictionary must be configured. For information on the specific Diameter dictionary to use, contact your Cisco account 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*>

  Important This command is obsolete in release 11.0 and later releases.
- *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. The Online/Offline AVP received at command level applies only to dynamic rules if they are not configured at PCC rule level.
  - 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 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 as described in Configuring Rel. 7 Gx Interface, on page 95.

```
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.
- For interpretation of the Gx rulebase (Charging-Rule-Base-Name AVP) from PCRF as 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 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 6: 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 }** This command is no longer an option in StarOS release 11.0 and beyond.

Rel. 8 Gx Interface

Rel. 8 Gx interface support is available on the Cisco ASR chassis 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.

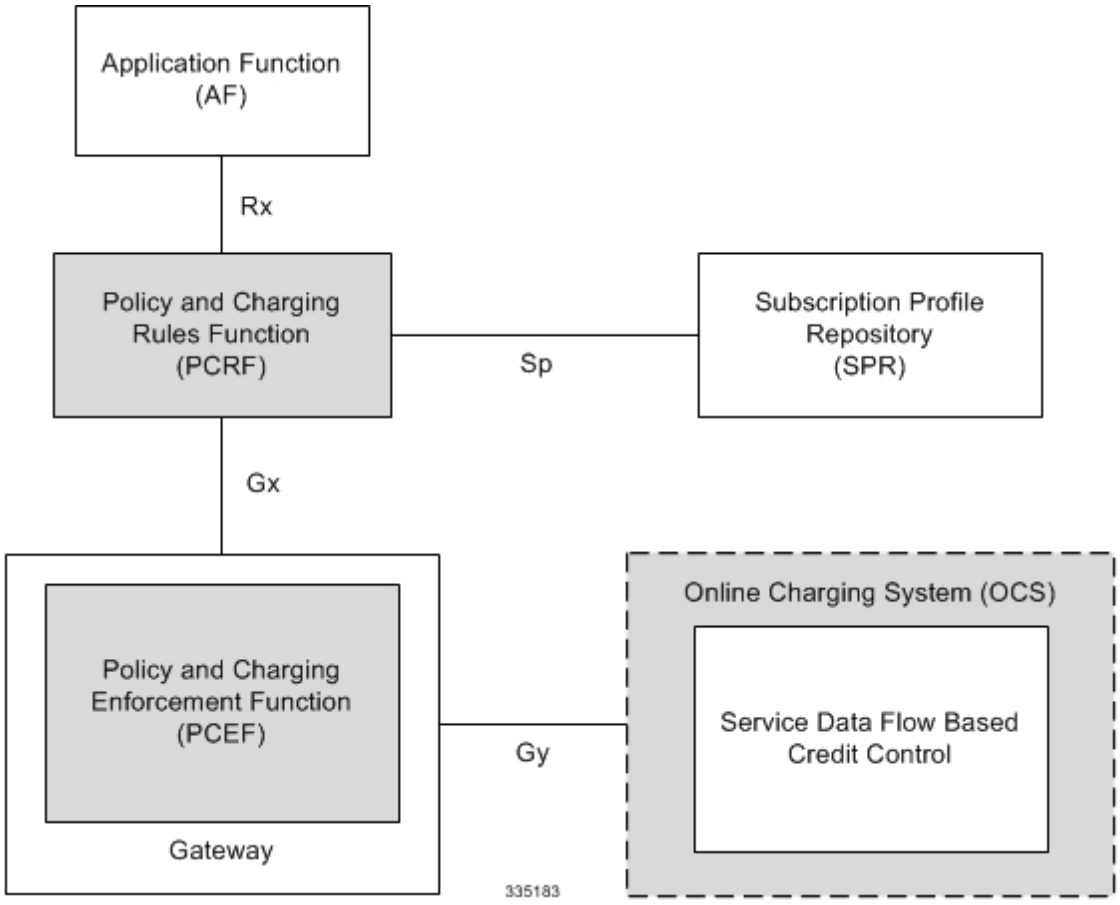
The PCC architecture allows operators to perform service-based QoS policy and FBC control. In the PCC architecture, this is accomplished mainly by the Policy and Charging Enforcement Function (PCEF)/HA/PDSN and the Policy and Charging Rules Function (PCRF). The client functionality lies with the HA/PDSN,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

Gx Interface Support

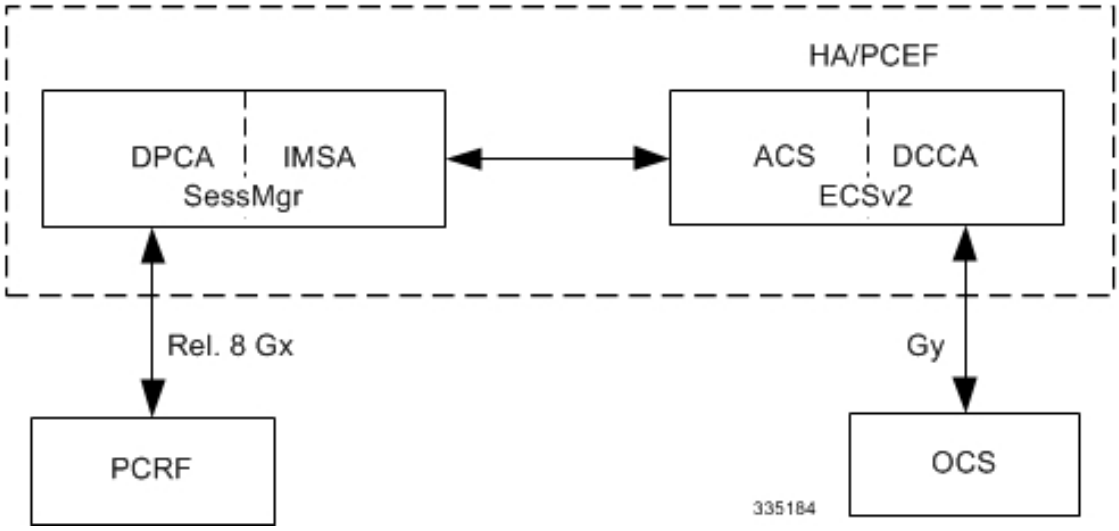
Figure 11: HA/PDSN Rel. 8 Gx PCC Logical Architecture



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



License Requirements

The HA/PDSN Rel. 8 Gx interface support is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

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 releases prior to 18, P-GW/GGSN does not send CCR-U with Charging Rule report for rule binding failure occurred during 4G to 3G HO in a collision case where create/update bearer response in 3G/4G is pending and update bearer of 3G HO is received. In 18 and later releases, CCR-U is generated and sent to PCRF for reporting rule failure when the collision happens during GnGp HO scenario.

This additional Gx message (CCR-U) triggered will require multiple CCR-Us to be configured when RAT_TYPE trigger is enabled. Otherwise, the subscriber call will be dropped whenever the collision happens during HO.

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.

In releases prior to 17.0, if "Rule-Deactivation-Time" AVP for a predefined rule was omitted in a CCA-U or RAR message, then any previous value for this AVP was continued to be used in the chassis. In 17.0 and later releases, if Rule-Deactivation-Time AVP is omitted in CCA/RAR, then any previous value for this AVP is no longer valid. The new behavior is compliant to the 3GPP specification for Gx, version 12.1.0.

If PCRF enables the same predefined rule again in RAR/CCA-U without Rule-Deactivation-Time AVP, then the deactivation-time for this rule, if any, will be removed.

For switching to the old behavior, PCRF should re-send the same value of Rule-Deactivation-Time AVP along with predef-rule name in the PCRF message (RAR, CCA-U).

Note This behavior change is applicable only to predefined rules.

Support for Firewall Policy on Gx

The Diameter AVP "SN-Firewall-Policy" has been added to the Diameter dynamic dictionary to support Firewall policy on Gx interface. This AVP can be encoded in CCA-I message to apply/overwrite the fw-and-nat policy that has either been statically assigned to the PDP context via APN configuration or dynamically assigned via RADIUS in Access-Accept. This AVP can also parsed in any CCA-U or RAR message to modify the fw-and-nat policy that is currently assigned to the PDP context.

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: 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. The Online/Offline AVP received at command level applies only to dynamic rules if they are not configured at PCC rule level.

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.

Gx Interface Support

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.

Important ASR 5500 supports only eight flow information including the flow description per dynamic charging rule in a Gx message.

In releases prior to 14.0, there were only 10 PCC rules that were recovered per bearer in the event of a session manager crash. In 14.0 and later releases, this limit has been increased to 24. That is, up to 24 PCC rules can be recovered post ICSR.

With the increase in the limit of PCC rules that can be recovered, the rules are not lost and hence the charging applied to the end users are not impacted.

In releases prior to 17.0, when P-GW received PCC rules from PCRF and it results in Create Bearer or Update Bearer to be triggered towards MME/S-GW, the PCC rules were kept in a pending-active state. Any modification request that was received for these pending-active rules were not currently honored by the P-GW.

In 17.0 and later releases, when modification for the PCC rules in pending-active state is received, the modified parameters will be buffered at P-GW. After the response for the pending request is received from the access network, P-GW will process the modification of the buffered parameters and if required generate another update towards network.

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.

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.

Releases prior to 14.0, when PCRF has subscribed to Out of Credit trigger, on session connect when one rule validation fails and also when an Out of Credit was received from OCS for another rule, P-GW was trying to report these failures in different CCR-U to PCRF. However, the second CCR-U of Out of credit was getting dropped internally.

In 14.0 and later releases, on session connect, P-GW combines the rule failure and out of credit in the same CCR-U and sends to PCRF.

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.

Important In 14.0 and later releases, the DPCA and the IMSA will be acting as one module within the Policy Server interface application.

Gx Interface Support

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

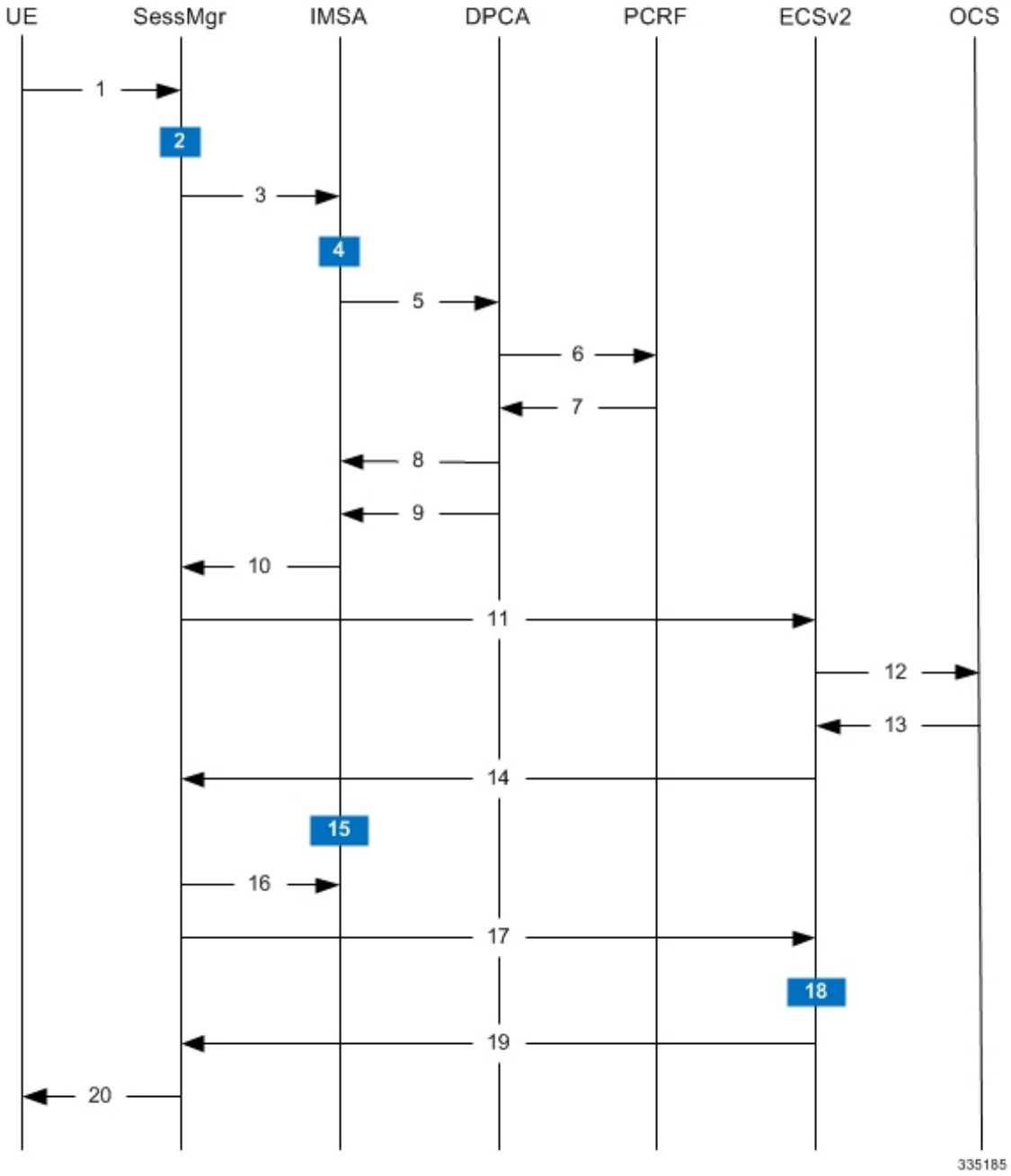


Table 7: HA/PDSN Rel. 8 Gx IMS Authorization Call flow Description

Step	Description
1	UE (IMS subscriber) requests for MIP Registration Request.
2	SessMgr allocates an IP address to the UE.

Step	Description
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.

Step	Description
15	SessMgr requests IMSA for the dynamic rules.
16	IMSA sends the dynamic rules to SessMgr. Note that, in 14.0 and later releases, the RAR messages are allowed before the session is established. In earlier releases, until the MIP session is established, all RAR messages from the PCRF were rejected. Also note that, in 14.0 and later releases, the RAR message is rejected and RAA is sent with 3002 result code when the recovery of dynamic rule information and audit of Session Manager are in progress. Earlier, the RAR messages were processed by DPCA even when the recovery audit was in progress.
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 Configuring IMS Authorization Service at Context Level, on page 115.

2. Within the same context, configure the subscriber template to use the IMSA service as described in Applying IMS Authorization Service to Subscriber Template, on page 116.
3. Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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.

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.
- In releases prior to 18, a maximum of 16 authorization services can be configured globally in the system. There is also a system limit for the maximum number of total configured services. In 18 and later releases, up to a maximum of 30 IMS authorization service profiles can be configured within the system.
- To enable Rel. 8 Gx interface support, pertinent Diameter dictionary must be configured. For information on the specific Diameter dictionary to use, contact your Cisco account 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 command.
- 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:

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

   context <*context_name*>

2. Verify the IMSA service 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 configured as described in Configuring IMS Authorization Service at Context Level, on page 115.

```
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.
- For interpretation of the Gx rulebase (Charging-Rule-Base-Name AVP) from PCRF as 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 8: 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**

Statistics/Information	Action to perform
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 }** This command is no longer an option in StarOS release 11.0 and beyond.

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 allows 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 allows 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 will 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 informs the PCRF about the mobility protocol tunnelling header of the service data flows at IP-CAN session establishment.

Terminology and Definitions

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

Volume Reporting Over Gx

This section describes the 3GPP Rel. 9 Volume Reporting over Gx feature.

License Requirements

The Volume Reporting over Gx is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Important In 12.0 and later releases, no separate license is required for Charging over Gx / Volume Reporting over Gx feature. This feature can be enabled as part of "Policy Interface" license.

Supported Standards

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

3GPP TS 29.212 V9.5.0 (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.

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.

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

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.

In 12.2 and later releases, usage reporting on bearer termination is supported.

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.

  In releases prior to 17.0, extra CCR-U was generated for a monitoring key when the following requests are received in the response to the CCR-U which reported the usage for the same monitoring key.

  - immediate reporting request with monitoring key at rule level
  - immediate reporting request with or without monitoring key at session level
  - explicit disable request at rule level
  - explicit disable request at session level

  In 17.0 and later releases, extra CCR-U is not generated for a monitoring key when all the above mentioned requests are received in the response to the CCR-U which reported the usage for the same monitoring key. Also, extra CCR-U is not generated when immediate reporting request without monitoring key at rule level is received in the response to the CCR-U which reported the usage for all the active monitoring keys.

- 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.

In releases prior to 15.0, when threshold breach happens for multiple monitoring keys at the same time, only one of the monitoring keys' usage is reported and the rest of the monitoring keys' usage is reported in CCR-T (threshold set to infinity). On Tx expiry/TCP link error, unreported usage is stored at ECS and reported only on session termination.

In 15.0 and later releases, only one of the monitoring keys' usage is reported first. Upon receiving successful response from PCRF, the rest of the monitoring keys' usage is reported to PCRF. On Tx expiry/TCP link error, unreported usage is stored at ECS. Any future successful interaction with PCRF for the session will send unreported UMI to PCRF.

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.

Gx Interface Support

- 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.

  PCRF uses RAR message and includes Session-Release-Cause AVP in it to initiate IP CAN Session Termination. However, there are some scenarios where PCRF may want to terminate the IP CAN Session in CCA messages. In order to avoid an unnecessary additional message, PCRF can inform P-GW to terminate the subscriber in CCA-U message itself. Hence, in 17.0 and later releases, the Session Release Cause has been added in CCA messages for all Gx dictionaries.

- 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.

  Releases prior to 14.0, when PCC rule was tried to be removed while waiting for access side update bearer response, the charging rules were not removed. In 14.0 and later releases, on receiving message from PCRF, the rule that is meant for removal is marked and then after the access side procedure is complete the rule is removed.

- 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.

- Release 12.2 onwards, usage reporting on bearer termination can be added. When a bearer is deleted due to some reason, the rules associated with the bearer will also be removed. So, the usage will be reported on the monitoring key(s) whose associated rule is the last one that is removed because of bearer termination.

- 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.

In releases prior to 17.0, CCR-U triggered on server retries does not take server granted quota into account for reporting USU. In 17.0 and later releases, CCR-U triggered on server retries takes server granted quota into account for reporting USU. For newly created MSCC, interim quota configuration is taken as reference for reporting USU.

For information on how to configure the Volume Reporting over Gx feature, refer to Configuring Volume Reporting over Gx, on page 99.

ICSR Support for Volume Reporting over Gx (VoRoGx)

In releases prior to 15.0, post the ICSR switchover, any existing session for which the PCRF has enabled volume reporting used to continue indefinitely until the session is terminated or until CCR-U is sent for a given trigger, without having the volume counted via Gx.

To summarize, after an ICSR switchover, volume reporting over Gx is no longer done for existing sessions. Also, volume usage is not synced to standby chassis.

In 15.0 and later releases, volume threshold and volume usage are synced to standby chassis to support volume reporting over Gx for existing sessions post switchover.

Without this support it cannot cause a subscriber to use higher speeds than what s/he is supposed to get, if volume reporting is for example used to enforce fair usage; the operator may already consider this a revenue loss. It will also severely impact roaming subscribers who are supposed to get a notification and be blocked/redirected once the limits set by the EU roaming regulation are reached. If a session continues now without being blocked, the operator is not allowed to charge for data beyond the limit and will have a significant and real revenue loss (roaming partner may still charge for the data used on their SGSNs).

Rel. 9 Gx Interface

Rel. 9 Gx interface support is available on the Cisco ASR chassis running StarOS 12.2 and later releases.

P-GW Rel. 9 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 allows 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 allows 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 reports to the PCRF when the status of the related service data flow changes.
- In case the SDF is tunnelled at the BBERF, the PCEF informs the PCRF about the mobility protocol tunnelling header of the service data flows at IP-CAN session establishment.

Important ASR 5500 supports only eight flow information including the flow description per dynamic charging rule in a Gx message.

Terminology and Definitions

This section describes features and terminology pertaining to Rel. 9 Gx functionality.

Volume Reporting Over Gx

This section describes the 3GPP Rel. 9 Volume Reporting over Gx feature.

License Requirements

The Volume Reporting over Gx is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Important In 12.0 and later releases, no separate license is required for Charging over Gx / Volume Reporting over Gx feature. This feature can be enabled as part of "Policy Interface" license.

Supported Standards

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

3GPP TS 29.212 V9.5.0 (2011-01): 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.

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.

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.

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

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.

In 12.2 and later releases, usage reporting on bearer termination is supported.

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.

In releases prior to 17.0, extra CCR-U was generated for a monitoring key when the following requests are received in the response to the CCR-U which reported the usage for the same monitoring key.

- immediate reporting request with monitoring key at rule level
- immediate reporting request with or without monitoring key at session level
- explicit disable request at rule level
- explicit disable request at session level

In 17.0 and later releases, extra CCR-U is not generated for a monitoring key when all the above mentioned requests are received in the response to the CCR-U which reported the usage for the same monitoring key. Also, extra CCR-U is not generated when immediate reporting request without monitoring key at rule level is received in the response to the CCR-U which reported the usage for all the active monitoring keys.

- 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.

In releases prior to 15.0, when threshold breach happens for multiple monitoring keys at the same time, only one of the monitoring keys' usage is reported and the rest of the monitoring keys' usage is reported in CCR-T (threshold set to infinity). On Tx expiry/TCP link error, unreported usage is stored at ECS and reported only on session termination.

In 15.0 and later releases, only one of the monitoring keys' usage is reported first. Upon receiving successful response from PCRF, the rest of the monitoring keys' usage is reported to PCRF. On Tx expiry/TCP link error, unreported usage is stored at ECS. Any future successful interaction with PCRF for the session will send unreported UMI to PCRF.

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.

  PCRF uses RAR message and includes Session-Release-Cause AVP in it to initiate IP CAN Session Termination. However, there are some scenarios where PCRF may want to terminate the IP CAN Session in CCA messages. In order to avoid an unnecessary additional message, PCRF can inform P-GW to terminate the subscriber in CCA-U message itself. Hence, in 17.0 and later releases, the Session Release Cause has been added in CCA messages for all Gx dictionaries.

- 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.

Releases prior to 14.0, when PCC rule was tried to be removed while waiting for access side update bearer response, the charging rules were not removed. In 14.0 and later releases, on receiving message from PCRF, the rule that is meant for removal is marked and then after the access side procedure is complete the rule is removed.

- 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.
- Release 12.2 onwards, usage reporting on bearer termination can be added. When a bearer is deleted due to some reason, the rules associated with the bearer will also be removed. So, the usage will be reported on the monitoring key(s) whose associated rule is the last one that is removed because of bearer termination.
- 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.

In releases prior to 17.0, CCR-U triggered on server retries does not take server granted quota into account for reporting USU. In 17.0 and later releases, CCR-U triggered on server retries takes server granted quota into account for reporting USU. For newly created MSCC, interim quota configuration is taken as reference for reporting USU.

For information on how to configure the Volume Reporting over Gx feature, see the Configuring Volume Reporting over Gx, on page 99 section.

ICSR Support for Volume Reporting over Gx (VoRoGx)

In releases prior to 15.0, post the ICSR switchover, any existing session for which the PCRF has enabled volume reporting used to continue indefinitely until the session is terminated or until CCR-U is sent for a given trigger, without having the volume counted via Gx.

To summarize, after an ICSR switchover, volume reporting over Gx is no longer done for existing sessions. Also, volume usage is not synced to standby chassis.

In 15.0 and later releases, volume threshold and volume usage are synced to standby chassis to support volume reporting over Gx for existing sessions post switchover.

Without this support it cannot cause a subscriber to use higher speeds than what s/he is supposed to get, if volume reporting is for example used to enforce fair usage; the operator may already consider this a revenue loss. It will also severely impact roaming subscribers who are supposed to get a notification and be blocked/redirected once the limits set by the EU roaming regulation are reached. If a session continues now without being blocked, the operator is not allowed to charge for data beyond the limit and will have a significant and real revenue loss (roaming partner may still charge for the data used on their SGSNs).

3GPP Rel.9 Compliance for IPFilterRule

This section describes the overview and implementation of 3GPP Rel.9 Compliance for IPFilterRule feature.

This section discusses the following topics for this feature:

- Feature Description, on page 129
- Configuring Rel.9 Compliant AVPs, on page 130
- Monitoring and Troubleshooting the 3GPP Rel.9 Compliance for IPFilterRule, on page 131

Feature Description

Currently, PCEF is 3GPP Rel. 8 compliant for IPFilterRule in Flow-Description AVP, TFT-Filter, and Packet-Filter-Content AVPs. When PCRF sends the CCA-U or RAR with Flow-Description AVP in Rel. 9 format during a network initiated dedicated bearer creation or modification, PCEF was misinterpreting the source and destination IP address, resulting in sending a wrong TFT to UE.

When the PCRF is upgraded to 3GPP Rel. 9, PCEF still sends CCR-U with Flow-Description, TFT-Filter and Packet-Filter-Content AVPs in Rel. 8 format during UE initiated secondary bearer creation or modification.

To make the PCEF 3GPP Rel. 9 compliant for Flow-Description AVP, TFT-Filter, and Packet-Filter-Content AVPs, the following changes are implemented:

- Interpretation of the source and destination IP address in IPFilterRule in Flow-Description AVP is changed to maintain 3GPP Rel.9 compliancy. That is, when a Rel. 9 Flow-Description for UPLINK is received during a network-initiated bearer creation or modification, the source IP address is interpreted as remote and the destination as local IP address.
- Traffic flow direction is interpreted from a new Diameter AVP "Flow-Direction". This new AVP indicates the direction or directions that a filter is applicable, downlink only, uplink only or both downlink and uplink (bi-directional).
- IMSA module is modified to encode TFT-Packet-Filter-Information and Packet-Filter-Information AVPs in Rel. 9 format if the negotiated supported feature is Rel. 9 and above.
- Configuration support is provided to enable Rel.9 changes for Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs sent by PCEF in CCR-U. The **diameter 3gpp-r9-flow-direction** CLI command is used to enable Rel. 9 changes. When this CLI command is configured and negotiated supported feature is Rel. 9 or above (both gateway and PCRF are Rel. 9+ compliant), P-GW sends Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs in Rel. 9 format.

Backward compatibility is maintained, i.e. both Rel. 8 (permit in/out) and Rel. 9 (permit out with flow-direction) formats are accepted by PCEF.

Per the 3GPP Rel. 8 standards, the IPFilterRule in Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs is sent as "permit in" for UPLINK and "permit out" for DOWNLINK direction. From 3GPP Rel. 9 onwards, the Flow-Description AVP within the Flow-Information AVP will have only "permit out" and the

traffic flow direction is indicated through Flow-Direction AVP. In 3GPP Rel. 9 format, both UPLINK and DOWNLINK are always sent as "permit out" and hence the usage of "permit in" is deprecated.

Important This feature is applicable for 3GPP Rel. 9 compliant PCEF and PCRF only when the supported feature negotiated in CCA-I is Rel. 9 or above through the **diameter update-dictionary-avps { 3gpp-r9 | 3gpp-r10 }** CLI command.

Relationships to Other Features

This feature works only when the **diameter update-dictionary-avps** CLI command is configured as 3gpp-r9 or 3gpp-r10. That is, PCEF will send Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs in 3GPP Rel. 9 format only when **diameter 3gpp-r9-flow-direction** CLI command is enabled and negotiated supported feature is Rel. 9 or above. The **diameter 3gpp-r9-flow-direction** CLI command for activating this feature must be used only after the PCRF is upgraded to Rel. 9.

Configuring Rel.9 Compliant AVPs

The following section provides the configuration commands to enable Rel.9 changes for Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs.

Encoding AVPs for 3GPP Compliance

Use the following configuration commands to control PCEF from sending Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs in Rel. 9 format.

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
            diameter 3gpp-r9-flow-direction
end
```

- **3gpp-r9-flow-direction**: Encodes Flow-Direction, Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs based on 3GPP Rel. 9 specification. By default, this feature is disabled.
- This CLI configuration is applicable only for TFT-Filter, Packet-Filter-Content, and Flow-Description AVPs sent by PCEF in CCR-U.
- This CLI command must be used only after the PCRF is upgraded to Rel. 9.
- This CLI command works in conjunction with **diameter update-dictionary-avps { 3gpp-r9 | 3gpp-r10 }**. When **diameter 3gpp-r9-flow-direction** is configured and negotiated supported feature is 3gpp-r9 or above, PCEF will send Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs in 3GPP Rel. 9 format.

Verifying the Configuration for AVP Compliance

Use the following command to verify the configuration status of this feature.

```
show ims-authorization service name service_name
```

service_name must be the name of the IMS Authorization service configured for IMS authentication.

The "3GPP R9 Flow Direction Compliance" field can be used to determine whether this feature is enabled or disabled.

```
[local]st40# show ims-authorization service name gngp-gx
  Context: gngp
  IMS Authorization Service name: gngp-gx
  Service State: Enabled
  Service Mode: Single Interface Policy and Charging
...
  Diameter Policy Control:
   Endpoint: gx
   Origin-Realm: xyz.com
   Dictionary: r8-gx-standard
   Supported Features:
      3gpp-r9
...
   Host Selection: Table: 1 Algorithm: Round-Robin
   Host Reselection Subscriber Limit: Not Enabled
   Host Reselection Interval: Not Enabled
   Sgsn Change Reporting: Not Enabled
    3GPP R9 Flow Direction Compliance: Enabled
  Host Selection Table[1]: 1 Row(s)
   Precedence: 1
...
```

Monitoring and Troubleshooting the 3GPP Rel.9 Compliance for IPFilterRule

This section provides information regarding show commands and/or their outputs in support of this feature.

The following operations should be performed for any failure related to this feature:

- Verify if the feature is enabled using **show ims-authorization service name** <*service_name*> CLI command. If not enabled, configure the **diameter 3gpp-r9-flow-direction** CLI command and check if it works.
- Execute **monitor protocol** command, and check if supported feature negotiated in CCA-I is Rel. 9 or above. If not, this feature will not work. Set the supported feature using **diameter update-dictionary-avps { 3gpp-r9 | 3gpp-r10 }** CLI command.
- If the failure is still observed, obtain the following information and contact Cisco account representative for further analysis:
  - monitor protocol log with options 24 (GTPC) and 75-3 (App Specific Diameter - DIAMETER Gx/Ty/Gxx) turned on
  - logs with acsmgr enabled
  - Output of **show active-charging sessions full all** and show ims-authorization sessions CLI commands

show ims-authorization service name

A new field "3GPP R9 Flow Direction Compliance" is added to the output of this show command to indicate whether the Rel. 9 Flow-Direction change is enabled or disabled.

Rel. 10 Gx Interface

Rel. 10 Gx interface support is available on the Cisco ASR chassis running StarOS 15.0 and later releases.

This section describes the following topic:

P-GW Rel. 10 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 allows 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 allows 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 will 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 informs the PCRF about the mobility protocol tunnelling header of the service data flows at IP-CAN session establishment.

Important ASR 5500 supports only eight flow information including the flow description per dynamic charging rule in a Gx message.

Terminology and Definitions

This section describes features and terminology pertaining to Rel. 10 Gx functionality.

Volume Reporting Over Gx

This section describes the 3GPP Rel. 10 Volume Reporting over Gx feature.

License Requirements

The Volume Reporting over Gx is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Important In 12.0 and later releases, no separate license is required for Charging over Gx / Volume Reporting over Gx feature. This feature can be enabled as part of "Policy Interface" license.

Supported Standards

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

3GPP TS 29.212 V10.5.0 (2012-01): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 10).

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.

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.

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

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.

In 12.2 and later releases, usage reporting on bearer termination is supported.

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.

In releases prior to 17.0, extra CCR-U was generated for a monitoring key when the following requests are received in the response to the CCR-U which reported the usage for the same monitoring key.

- immediate reporting request with monitoring key at rule level
- immediate reporting request with or without monitoring key at session level
- explicit disable request at rule level
- explicit disable request at session level

In 17.0 and later releases, extra CCR-U is not generated for a monitoring key when all the above mentioned requests are received in the response to the CCR-U which reported the usage for the same monitoring key. Also, extra CCR-U is not generated when immediate reporting request without monitoring key at rule level is received in the response to the CCR-U which reported the usage for all the active monitoring keys.

- 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.

In releases prior to 15.0, when threshold breach happens for multiple monitoring keys at the same time, only one of the monitoring keys' usage is reported and the rest of the monitoring keys' usage is reported in CCR-T (threshold set to infinity). On Tx expiry/TCP link error, unreported usage is stored at ECS and reported only on session termination.

In 15.0 and later releases, only one of the monitoring keys' usage is reported first. Upon receiving successful response from PCRF, the rest of the monitoring keys' usage is reported to PCRF. On Tx expiry/TCP link error, unreported usage is stored at ECS. Any future successful interaction with PCRF for the session will send unreported UMI to PCRF.

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.

  PCRF uses RAR message and includes Session-Release-Cause AVP in it to initiate IP CAN Session Termination. However, there are some scenarios where PCRF may want to terminate the IP CAN Session in CCA messages. In order to avoid an unnecessary additional message, PCRF can inform P-GW to

Gx Interface Support

terminate the subscriber in CCA-U message itself. Hence, in 17.0 and later releases, the Session Release Cause has been added in CCA messages for all Gx dictionaries.

- 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.

  Releases prior to 14.0, when PCC rule was tried to be removed while waiting for access side update bearer response, the charging rules were not removed. In 14.0 and later releases, on receiving message from PCRF, the rule that is meant for removal is marked and then after the access side procedure is complete the rule is removed.

- 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.

- Release 12.2 onwards, usage reporting on bearer termination can be added. When a bearer is deleted due to some reason, the rules associated with the bearer will also be removed. So, the usage will be reported on the monitoring key(s) whose associated rule is the last one that is removed because of bearer termination.

- 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.

In releases prior to 17.0, CCR-U triggered on server retries does not take server granted quota into account for reporting USU. In 17.0 and later releases, CCR-U triggered on server retries takes server granted quota into account for reporting USU. For newly created MSCC, interim quota configuration is taken as reference for reporting USU.

For information on how to configure the Volume Reporting over Gx feature, refer to Configuring Volume Reporting over Gx, on page 99.

ICSR Support for Volume Reporting over Gx (VoRoGx)

In releases prior to 15.0, post the ICSR switchover, any existing session for which the PCRF has enabled volume reporting used to continue indefinitely until the session is terminated or until CCR-U is sent for a given trigger, without having the volume counted via Gx.

To summarize, after an ICSR switchover, volume reporting over Gx is no longer done for existing sessions. Also, volume usage is not synced to standby chassis.

In 15.0 and later releases, volume threshold and volume usage are synced to standby chassis to support volume reporting over Gx for existing sessions post switchover.

Without this support it cannot cause a subscriber to use higher speeds than what s/he is supposed to get, if volume reporting is for example used to enforce fair usage; the operator may already consider this a revenue loss. It will also severely impact roaming subscribers who are supposed to get a notification and be blocked/redirected once the limits set by the EU roaming regulation are reached. If a session continues now without being blocked, the operator is not allowed to charge for data beyond the limit and will have a significant and real revenue loss (roaming partner may still charge for the data used on their SGSNs).

Use of the Supported-Features AVP on the Gx Interface

The Supported-Features AVP is used during session establishment to inform the destination host about the required and optional features that the origin host supports. The client will, in the first request in a Diameter session indicate the set of features required for the successul processing of the session. If there are features supported by the client that are not advertised as part of the required set of features, the client will provide in the same request this set of optional features that are optional for the successful processing of the session. The server will, in the first answer within the Diameter session indicate the set of features that it has in common with the client and that the server will support within the same Diameter session. Any further command messages will always be compliant with the list of supported features indicated in the Supported-Features AVPs and features that are not indicated in the Supported-Features AVPs during session establishment. Features that are not advertised as supported will not be used to construct the command messages for that Diameter session. Unless otherwise stated, the use of the Supported-Features AVP on the Gx reference point will be compliant with the requirements for dynamic discovery of supported features and associated error handling.

The base functionality for the Gx reference point is the 3GPP Rel. 7 standard and a feature is an extension to that functionality. If the origin host does not support any features beyond the base functionality, the Supported-Features AVP may be absent from the Gx commands. As defined in 3GPP TS 29.229, when extending the application by adding new AVPs for a feature, the new AVPs will have the M bit cleared and the AVP will not be defined mandatory in the command ABNF.

The Supported-Features AVP is of type grouped and contains the Vendor-Id, Feature-List-ID and Feature-List AVPs. On the Gx reference point, the Supported-Features AVP is used to identify features that have been defined by 3GPP and hence, the Vendor-Id AVP will contain the vendor ID of 3GPP (10415). If there are multiple feature lists defined for the Gx reference point, the Feature-List-ID AVP will differentiate those lists from one another.

Feature bit	Feature	M/O	Description
0	Rel8	M	This feature indicates the support of base 3GPP Rel-8 Gx functionality, including the AVPs and corresponding procedures supported by the base 3GPP Rel-7 Gx standard, but excluding those features represented by separate feature bits.
1	Rel9	M	This feature indicates the support of base 3GPP Rel-9 Gx functionality, including the AVPs and corresponding procedures supported by the Rel8 feature bit, but excluding those features represented by separate feature bits.
3	Rel10	M	This feature indicates the support of base 3GPP Rel-10 Gx functionality, including the AVPs and corresponding procedures supported by the Rel8 and Rel9 feature bit, but excluding those features represented by separate feature bits.
4	SponsoredConnectivity	O	This feature indicates support for sponsored data connectivity feature. If the PCEF supports this feature, the PCRF may authorize sponsored data connectivity to the subscriber.

In releases prior to 15.0, the Supported-Features AVP was not encoded in CCR-U messages, but it was supported only in CCR-I message. If Rel. 8 dictionary or any dictionary beyond Rel. 8 is used and PCRF does not provide Supported-Features AVP in CCA-I, then the call gets dropped.

In 15.0 and later releases, if PCEF configures Diameter dictionary as release 8, 9 or 10, then PCRF sends Supported-Features AVP so that PCEF will know what feature PCRF supports. If PCEF receives supported features lesser than or greater than requested features then supported feature will be mapped to the lower one.

Whenever the custom dictionary "dpca-custom24" is configured, the Supported-Features AVP including Vendor-Id AVP will be sent in all CCR messages.

Rule-Failure-Code AVP

The Rule-Failure-Code AVP indicates the reason that the QoS/PCC rules cannot be successfully installed/activated or enforced. The Rule-Failure-Code AVP is of type Enumerated. It is sent by the PCEF to the PCRF within a Charging-Rule-Report AVP to identify the reason a PCC Rule is being reported.

In releases prior to 15.0, only 11 rule failure codes were defined as the values for this AVP. In 15.0 and later releases, two new rule failure codes INCORRECT_FLOW_INFORMATION (12) and NO_BEARER_BOUND (15) are added. The name of the existing rule failure code 9 is changed to MISSING_FLOW_INFORMATION. For 3GPP Rel. 10, rule failure code 9 maps to GW/PCEF_MALFUNCTION.

Sponsored Data Connectivity

With Sponsored Data Connectivity, the sponsor has a business relationship with the operator and the sponsor reimburses the operator for the user's data connectivity in order to allow the user access to an associated Application Service Provider's (ASP) services. Alternatively, the user pays for the connectivity with a transaction which is separate from the subscriber's charging. It is assumed the user already has a subscription with the operator.

Sponsored Data Connectivity feature is introduced in Rel. 10 of 3GPP TS 29.212 specification. If Sponsored Data Connectivity is supported, the sponsor identity for a PCC rule identifies the 3rd party organization (the sponsor) who is willing to pay for the operator's charge for connectivity required to deliver a service to the end user.

The purpose of this feature is to identify the data consumption for a certain set of flows differently and charge it to sponsor. To support this, a new reporting level "SPONSORED_CONNECTIVITY_LEVEL" is added for reporting at Sponsor Connection level and two new AVPs "Sponsor-Identity" and "Application-Service-Provider-Identity" have been introduced at the rule level.

Sponsored Data Connectivity will be performed for service data flows associated with one or more PCC rules if the information about the sponsor, the application service provider and optionally the threshold values are provided by the Application Function (AF).

The provisioning of sponsored data connectivity per PCC rule will be performed using the PCC rule provisioning procedure. The sponsor identity will be set using the Sponsor-Identity AVP within the Charging-Rule-Definition AVP of the PCC rule. The application service provider identity will be set using the Application-Service-Provider-Identity AVP within the Charging-Rule-Definition AVP of the PCC rule. Sponsor-Identity AVP and Application-Service-Provider-Identity AVP will be included if the Reporting-Level AVP is set to the value SPONSORED_CONNECTIVITY_LEVEL.

When receiving the flow based usage thresholds from the AF, the PCRF will use the sponsor identity to generate a monitoring key. The PCRF may also request usage monitoring control, in this case, only the flow based usage is applied for the sponsored data connectivity. If requested, the PCEF may also report the usage to the PCRF.

A new CLI command "**diameter encode-supported-features**" has been added in Policy Control Configuration mode to send supported features with Sponsor Identity. For more information on the command, see the *Command Line Interface Reference*.

Sponsored connectivity feature will be supported only when both P-GW and PCRF support 3GPP Rel. 10. P-GW advertises release as a part of supported features in CCR-I to PCRF. If P-GW supports Release 10 and also sponsored connectivity but PCRF does not support it (as a part of supported features in CCA-I), this feature will be turned off.

This feature implementation impacts only the Gx dictionary "dpca-custom15". Also note that this feature is supported only for the dynamic rules.

Volume Reporting

For Volume Reporting over Gx, PCRF generates a unique monitoring key based on sponsor identity. Since flows with different monitoring keys are treated differently, flows with sponsor ID are charged differently.

Supported Gx Features

Assume Positive for Gx

In a scenario where both the primary and secondary PCRF servers are overloaded, the PCRF returns an error to P-GW and HSGW. Current behavior for the P-GW and HSGW is to terminate the session if both primary and secondary return a failure or timeout.

This feature is developed to enhance this behavior by applying local policy on the GW to ensure that the subscriber session continues. P-GW / HSGW should implement Assume Positive feature to handle errors and based on the event type implement specific rules.

Important Use of Gx Assume Positive requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

The failure handling behavior is enhanced to ensure that the subscriber service is maintained in case of PCRF unavailability. It is also required that the GW reduces the traffic towards the PCRF when receiving a Diameter Too Busy (3004) by stopping the transmission and reception of Diameter messages (CCRs and RARs) to and from the PCRF for a configurable amount of time.

In case of any of the following failures with PCRF, the GW chooses to apply failure handling which results in subscriber termination or to allow browsing without any more policy enforcement.

- TCP link failure
- Application Timer (Tx) expiry
- Result code based failures

In 14.1 and later releases, the PCRF is allowed to fall back to Local Policy for all connection level failures, result code/experimental result code failures. Local Policy may choose to allow the subscriber for a configured amount of time. During this time any subscriber/internal event on the call would be handled from Local Policy. After the expiry of the timer, the subscriber session can be either terminated or else PCRF can be retried. Note that the retry attempt to PCRF happens only when the **timer-expiry event** is configured as **reconnect-to-server**.

The fallback support is added to the failure handling template and the local policy service needs to be associated to IMS Authorization service.

Once the local policy is applied, all PCRF enabled event triggers will be disabled. When the subscriber session is with the local-policy, the GW skips sending of CCR-T and cleans up the session locally.

For a session that was created with active Gx session, the GW sends the CCR-T to primary and on failure sends the CCR-T to the secondary PCRF. If the CCR-T returns a failure from both primary and secondary or times out, the GW cleans up the session locally.

Fallback to Local Policy is done in the following scenarios:

- Tx timer expiry
- Diabase Error

- Result Code Error (Permanent/Transient)
- Experimental Result Code
- Response Timeout

The following points are applicable only in the scenario where reconnect to PCRF is attempted.

- If the subscriber falls back to local-policy because of CCR-I failure, CCR-I will be sent to the PCRF after the timer expiry. On successful CCA-I call will be continued with PCRF or else the call will be continued with local-policy and retry-count will be incremented.
- If the subscriber falls back to local-policy because of the CCR-U failure, IMS Authorization application waits for some event change to happen or to receive an RAR from PCRF.
- In case of event change after the timer expiry, CCR-U will be sent to PCRF. On successful CCA-U message, call will be continued with PCRF or else call will be with local-policy and retry-count will be incremented.
- If RAR is received after the timer-expiry the call will be continued with the PCRF. On expiry of maximum of retries to connect to PCRF, call will be disconnected.

Default Policy on CCR-I Failure

The following parameters are supported for local configuration on P-GW. The configuration parameters are configurable per APN and per RAT Type.

The following fields for a Default Bearer Charging Rule are configurable per APN and per RAT Type:

- Rule Name
- Rating Group
- Service ID
- Online Charging
- Offline Charging
- QCI
- ARP
  - Priority Level
  - QCI
  - QVI
- Max-Requested-Bandwidth
  - UL
  - DL

Flow Description and Flow Status are not configurable but the default value will be set to Any to Any and Flow Status will be set to Enabled.

The following command level fields are configurable per APN and per RAT Type:

- AMBR
  - UL
  - DL
- QCI
- ARP

- Priority Level
- QCI
- QVI

Gx Back off Functionality

This scenario is applicable when Primary PCRF cluster is unavailable but the secondary PCRF is available to handle new CCR-I messages.

When the chassis receives 3004 result-code then back-off timer will be started for the peer and when the timer is running no messages will be sent to that peer.

The timer will be started only when the value is being configured under endpoint configuration.

Releases prior to 15.0, when the IP CAN session falls back to local policy it remained with local policy until the termination timer expires or the subscriber disconnects. Also, the RAR message received when the local-policy timer was running got rejected with the cause "Unknown Session ID".

In 15.0 and later releases, P-GW/GGSN provides a fair chance for the subscriber to reconnect with PCRF in the event of CCR failure. To support this feature, configurable validity and peer backoff timers are introduced in the Local Policy Service and Diameter endpoint configuration commands. Also, the RAR received when the local-policy timer is running will be rejected with the cause "DIAMETER_UNABLE_TO_DELIVER".

In releases prior to 17.0, rule report was not sent in the CCR messages when PCRF is retried after the expiry of validity timer. In 17.0 and later releases, rule report will be sent to the PCRF during reconnect when the CLI command **diameter encodeevent-avps local-fallback** is configured under Policy Control Configuration mode.

Support for Volume Reporting in Local Policy

This feature provides support for time based reconnect to PCRF instead of the event based for CCR-U failure scenarios.

In releases prior to 17.0, the following behaviors were observed with respect to the Volume Reporting for Local Policy:

- In the event of CCR-U failure, CCR-U was triggered to PCRF only on receiving subscriber event.
- When a CCR-U failure happened and a call continued without Gx, unreported volume is lost as the threshold is set to infinity. In next CCR-U triggered to PCRF, the cumulative volume was sent to PCRF.
- RAR was rejected with result-code diameter_unable_to_comply (3002) when the validity timer is running.

In 17.0 and later releases, with the timer-based implementation, this feature introduces the following changes to the existing behavior:

- When send-usage-report is configured, the CCR-U with usage report will be sent immediately after the local-policy timer-expiry.
- The unreported usage will not be returned to ECS. Thus, usage since last tried CCR-U will be sent to PCRF.
- RAR will be accepted and the rules received on RAR will be installed even when the timer is running.

Session can be connected to PCRF immediately instead of waiting for subscriber event, and the updated usage report can be sent.

Support for Session Recovery and Session Synchronization

Currently PCRF and ASR 5500 gateway node are in sync during normal scenarios and when Gx assume positive is not applied. However, there are potential scenarios where the PCRF might have been locally deleted or lost the Gx session information and it is also possible that due to the loss of message, gateway node and PCRF can be out of sync on the session state.

While these are rare conditions in the network, the desired behavior is to have PCRF recover the Gx session when it is lost and also to have PCRF and gateway sync the rule and session information. This feature provides functionality to ensure PCRF and gateway can sync on session information and recover any lost Gx sessions. Configuration support has been provided to enable session recovery and session sync features.

In releases prior to 17.0, the implementation is as follows:

- If the PCRF deletes or loses session information during a Gx session update (CCR-U) initiated by the gateway, PCRF will respond back with DIAMETER_UNKNOWN_SESSION_ID resulting in session termination even in the case of CCR-U.
- If the PCRF deletes or loses session information and an Rx message is received, PCRF will not be able to implement corresponding rules and will result in failure of subscriber voice or video calls.
- For subscriber's existing Rx sessions and active voice/video calls, PCRF will not be able to initiate cleanup of the sessions towards the gateway and can result in wastage of the resources in the network (dedicated bearers not removed) or can result in subscriber not able to place calls on hold or conference or remove calls from hold.
- For out of sync scenarios, PCRF and gateway could be implementing different policies and can result in wastage of resources or in poor subscriber experience. Existing behavior does not provide for a way to sync the entire session information.

In 17.0 and later releases, the gateway (GW) node and PCRF now supports the ability to exchange session information and the GW provides the complete subscriber session information to enable PCRF to build the session state. This will prevent the occurrence of the above mentioned scenarios and ensure that GW and PCRF are always in sync. The keywords **session-recovery** and **session-sync** are used with the **diameter encode-supported-features** CLI command in Policy Control Configuration mode to support Gx Synchronization.

Configuring Gx Assume Positive Feature

To configure Gx Assume Positive functionality:

Step 1 At the global configuration level, configure Local Policy service for subscribers as described in the Configuring Local Policy Service at Global Configuration Level, on page 144.

Step 2 At the global configuration level, configure the failure handling template to use the Local Policy service as described in the Configuring Failure Handling Template at Global Configuration Level, on page 145.

Step 3 Within the IMS Authorization service, associate local policy service and failure handling template as described in the Associating Local Policy Service and Failure Handling Template, on page 145.

Step 4 Verify your configuration as described in the Verifying Local Policy Service Configuration, on page 145.

Step 5 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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.

Configuring Local Policy Service at Global Configuration Level

Use the following example to configure Local Policy Service at global configuration level for subscribers:

```
configure
    local-policy-service  LOCAL_PCC
          ruledef 2G_RULE
               condition priority 1 apn match .*
               exit
          ruledef all-plmn
               condition priority 1 serving-plmn match .*
               exit
          actiondef 2G_UPDATE
               action priority 1 activate-ambr uplink 18000 downlink 18000
               action priority 2 reject-requested-qos
               exit
          actiondef action1
               action priority 2 allow-requested-qos
               exit
          actiondef allow
               action priority 1 allow-session
               exit
          actiondef delete
               action priority 1 terminate-session
               exit
          actiondef lp_fall
               action priority 1 reconnect-to-server
               exit
          actiondef time
               action priority 1 start-timer timer duration 10
          exit
          eventbase default
               rule priority 1 event fallback ruledef 2G_RULE actiondef time
 continue
             rule priority 2 event new-call ruledef 2G_RULE actiondef action1

            rule priority 3 event location-change ruledef 2G_RULE actiondef
action1
               rule priority 5 event timer-expiry ruledef 2G_RULE actiondef
lp_fall
              rule priority 6 event request-qos default-qos-change ruledef
2G_RULE actiondef allow
               end
```

Notes:

- On occurrence of some event, event will be first matched based on the priority under the eventbase default. For the matched rule and if the corresponding ruledef satisfies, then specific action will be taken.

Configuring Failure Handling Template at Global Configuration Level

Use the following example to configure failure handling template at global configuration level:

```
configure
   failure-handling-template <template_name>
      msg-type any failure-type any action continue local-fallback
      end
```

Notes:

- When the TCP link failure, Application Timer (Tx) expiry, or Result code based failure happens, the associated failure-handling will be considered and if the failure-handling action is configured as local-fallback, then call will fall back to local-fallback mode.

Associating Local Policy Service and Failure Handling Template

Use the following example to associate local policy service and failure handling template:

```
configure
   context <context_name>
      ims-auth-service <service_name>
         associate local-policy-service <lp_service_name>
         associate failure-handling <failure-handling-template-name>
         end
```

Verifying Local Policy Service Configuration

To verify the local policy service configuration, use this command:

```
show local-policy statistics service service_name
```

Time Reporting Over Gx

This section describes the Time Reporting over Gx feature supported for GGSN in this release.

License Requirements

No separate license is required for Time Reporting over Gx feature. This feature can be enabled as part of "Policy Interface" license.

Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Feature Overview

This non-standard Time Usage Reporting over Gx feature is similar to Volume Usage Reporting over Gx. PCRF provides the time usage threshold for entire session or particular monitoring key in CCA or RAR. When the given threshold breached usage report will be sent to PCRF in CCR. This time threshold is independent of data traffic. Apart from the usage threshold breach there are other scenarios where usage report will be send to PCRF.

Important Time reporting over Gx is applicable only for time quota.

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

If the time 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.

Time usage reporting on bearer termination is supported. When a bearer is deleted due to some reason, the rules associated with the bearer will also be removed. So, the usage will be reported on the monitoring key(s) whose associated rule is the last one that is removed because of bearer termination.

The following steps explain how Time Reporting over Gx works:

1. PCEF after receiving the message from PCRF parses the time monitoring related AVPs, and sends the information to IMSA.
2. IMSA updates the information to ECS.
3. Once the ECS is updated with the time monitoring information from PCRF, the PCEF (ECS) starts tracking the time usage.
4. For session-level monitoring, the ECS maintains the amount of time usage.
5. For PCC rule monitoring, usage is monitored with the monitoring key as the unique identifier. Each node maintains the time usage information per monitoring key.
6. The PCEF continues to track time 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 time monitoring does not continue in the PCEF for that IP CAN session.

Limitations

This section lists the limitations for Time Reporting over Gx in this release.

- Only integer monitoring key will be supported like Volume Reporting over Gx
- If the same monitoring key is used for both time and data volume monitoring then disabling monitoring key will disable both time and data usage monitoring.
- If the same monitoring key is used for both time and data usage monitoring and if an immediate report request is received, then both time and volume report of that monitoring key will be sent.

Usage Monitoring

Two levels of time usage reporting are supported:

- Usage Monitoring at Session Level
- Usage Monitoring at Flow Level

Usage Monitoring at Session Level

PCRF subscribes to the session level time 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).

Usage Monitoring at Flow Level

PCRF subscribes to the flow level time 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 or disabling of usage monitoring at flow level can be controlled by PCRF using it. Usage monitoring is supported for both predefined rules and dynamic rule definition.

Usage Monitoring for Predefined and Static 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 time being tracked for multiple rules having the same monitoring key. Similarly, usage monitoring information is sent from PCRF for the static rules also.

Usage Monitoring for Dynamic Ruledefs

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 results in the usage monitoring being done for all the rules associated with that monitoring key.

Usage Reporting

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

- Usage Threshold Reached: PCEF records the subscriber usage and checks if the usage threshold provided by PCRF is reached. 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 PCRF. The Usage-Monitoring-Information AVP is sent in this CCR with the "CC-Time" in "Used-Service-Unit" set to track the time usage of the subscriber.
- Usage Monitoring Disabled: If PCRF explicitly disables the usage monitoring with Usage-Monitoring-Support AVP set to USAGE_MONITORING_DISABLED, 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.
- 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.

  PCRF uses RAR message and includes Session-Release-Cause AVP in it to initiate IP CAN Session Termination. However, there are some scenarios where PCRF may want to terminate the IP CAN Session in CCA messages. In order to avoid an unnecessary additional message, PCRF can inform P-GW to terminate the subscriber in CCA-U message itself. Hence, in 17.0 and later releases, the Session Release Cause has been added in CCA messages for all Gx dictionaries.
- PCC Rule Removal: When the PCRF deactivates the last PCC rule associated with a usage monitoring key, PCEF sends a CCR with the usage time 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.

- PCRF Requested Usage Report: When PCRF provides the Usage-Monitoring-Information with the Usage-Monitoring-Report set to USAGE_MONITORING_REPORT_REQUIRED, PCEF sends the time usage information. If the monitoring key is provided by PCRF, time usage for that monitoring key is notified to PCRF regardless of usage threshold. If the monitoring key is not provided by PCRF, time usage for all enabled monitoring keys is notified to PCRF.
- Event Based Reporting: The event based reporting can be enabled through the CLI command **event-update send-usage-report events**. When an event like sgsn change, qos change or revalidation-timeout is configured under this CLI, time usage report is generated whenever that event happens.

Once the usage is reported, the usage counter is reset to zero. The PCEF continues to track time 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 time usage monitoring does not continue in the PCEF for that IP CAN session.

For information on how to configure the Time Reporting over Gx feature, see the Configuring Time Reporting over Gx, on page 148.

Configuring Time Reporting over Gx

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

To enable Time 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 configuration for enabling Time Reporting over Gx is same as the Volume Reporting over Gx configuration. If a time threshold is received from PCRF then Time monitoring is done, and if a volume threshold is received then Volume monitoring will be done.
- 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 enables time usage report to be sent in event updates. 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 time usage information as part of event update but not reset at PCEF.

Support for Multiple Active and Standby Gx Interfaces to PCRF

In the earlier Gx implementation, Diameter Policy Control Application has the limitation to mandatorily configure hosts as part of IMS Authorization service or associate a host template and select the hosts to be communicated for each subscriber session. Since the peer selection can happen at diabase and application need not select any hosts, this feature is developed to remove the restrictions imposed in the application and allow diabase to pick the peers in a round robin fashion. In addition, this feature will take care of peer selection at diabase even when the hosts picked by application are not active. This change in behavior is controlled through the CLI command "**endpoint-peer-select**" as the default behavior is to drop the call if the server discovery fails at application.

When the call is established, IMSA module checks the host selection table/prefix table/host template associated in IMSA service to pick the primary and secondary peers to be contacted. If no host table/prefix table/host template is configured or none of the rows in prefix table are matching or the hosts selected by IMSA are inactive, then based on the CLI configuration the control is given to diabase module which will select the peers in a round robin fashion or terminate the call based on the CLI configuration.

When the CCR message results in a diabase error/Tx expiry/response timeout, then IMSA will let diabase select an alternate route by excluding the peer which resulted in the failure and switch to the peer if the lookup is successful.

When CCR/CCA message is exchanged with the directly connected host selected by diabase and RAR message is received from new host, then IMSA will skip host configuration check and let further communication to happen with the new host. If the directly connected host is selected by application during call establishment, then IMSA will check if the new host is the secondary server per application. When the CCR/CCA message is exchanged with indirectly connected host through DRA which is picked by diabase and RAR message is received from same host through another DRA, then IMSA will skip host configuration check and let further communication to happen with the same host through the new DRA. If the DRA is selected by application during call establishment, then IMSA will check if the new DRA is the secondary server per application. Even if RAR message is received from different host though another DRA, IMSA will skip host configuration check and let further communication to happen with the new host through the new DRA.

Configuring Diameter Peer Selection at Diabase in Failure Scenarios

The following configuration enables diabase to select the Diameter peers when IMSA fails.

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
            endpoint-peer-select [ on-host-select-failure |
on-inactive-host ]
            { default | no } endpoint-peer-select
            end
```

Notes:

- This command is used to perform server selection at diabase when the hosts could not be selected by IMS Authorization application or when the hosts selected by the IMS Authorization application is inactive. For example, host table is not configured in IMSA service, host table is configured but not activated, none of the rows in prefix table match the subscriber, host template is not associated with IMSA service, host template could not select the hosts.
- **on-host-select-failure**: Specifies to perform server selection at Diabase when the hosts could not be selected by IMS Authorization application.

- **on-inactive-host**: Specifies to perform server selection at diabase when the hosts selected by application are inactive.
- This CLI command is added in policy control configuration mode to maintain backward compatibility with the old behavior of terminating the call when server selection fails at IMS Authorization application.

Support for Multiple CCR-Us over Gx Interface

ASR 5500 node earlier supported only one pending CCR-U message per session over Gx interface. Any request to trigger CCR-U (for access side updates/internal updates) were ignored/dropped, when there was already an outstanding message pending at the node. PCEF and PCRF were out of synch if CCR-U for critical update was dropped (like RAT change/ULI change).

In 17.0 and later releases, ASR 5500 supports multiple CCR-U messages at a time per session through the use of a configurable CLI command "**max-outstanding-ccr-u**" under IMS Authorization Service configuration mode. That is, this CLI will allow the user to configure a value of up to 12 as the maximum number of CCR-U messages per session.

The CLI-based implementation allows sending request messages as and when they are triggered and processing the response when they are received. The gateway does re-ordering if the response messages are received out of sequence.

To support multiple outstanding messages towards PCRF, the following items should be supported:

- Allowing IMSA to send multiple CCR-U messages – This can be achieved through the use of **max-outstanding-ccr-u** command in the IMS Authorization Service configuration mode.
- Queuing of response message for ordering – DPCA should parse the received message irrespective of order in which they are received. IMSA will check whether to forward the response to session manager or queue it locally.
- Peer switch – When multiple CCR-Us are triggered, IMSA will start Tx timer for each request sent out. On first Tx expiry, IMSA/DPCA will do peer switch. That is, IMSA will stop all other requests' Tx timers and switch to secondary peer (if available) or take appropriate failure handling action.
- Failure handling – On peer switch failure due to Tx expiry, DPCA will take failure handling action based on the configuration present under ims-auth-service.
- Handling back pressure – In case of multiple CCR-Us triggered to Primary PCRF and due to Tx timeout all the messages are switched to Secondary PCRF. If Secondary server is already in backpressure state, then IMSA will put first message in the backpressure queue and once after message is processed next pending request will be put into BP queue.
- Volume reporting – In case of multiple CCR-Us for usage report is triggered (for different monitoring keys) and failure handling is configured as "**continue send-ccrt-on-call-termination**", on first Tx timeout or response timeout, usage report present in all the CCR-Us will be sent to ECS. All the unreported usage will be sent in CCR-T message when the subscriber goes down. If "**event-update send-usage-report**" CLI is present, then there are chances of reporting usage for same monitoring key in multiple CCR-Us.

Though the **max-outstanding-ccr-u** CLI command supports configuring more than one CCR-U, only one outstanding CCR-U for access side update is sent out at a time and multiple CCR-Us for internal updates are sent.

These are the access side updates for which CCR-U might be triggered:

- Bearer Resource Command
- Modify Bearer Request (S-GW change, RAT change, ULI change)
- Modify Bearer Command

These are the following internal updates for which CCR-U is triggered:

- S-GW restoration
- Bearer going down (GGSN, BCM UE_Only)
- ULI/Timezone notification
- Default EPS bearer QoS failure
- APN AMBR failure
- Charging-Rule-Report
- Out of credit / reallocation of credit
- Usage reporting
- Tethering flow detection
- Access network charging identifier

Configuring Gateway Node to Support Back-to-Back CCR-Us

The following configuration enables or disables the gateway to send multiple back-to-back CCR-Us to PCRF.

```
configure
   context  context_name
      ims-auth-service   service_name
         policy-control
            [ default ] max-outstanding-ccr-u value
            end
```

Notes:

- *value* must be an integer value from 1 through 12. The default value is 1.

Support for RAN/NAS Cause IE on Gx Interface

New supported feature "Netloc-RAN-NAS-Cause" has been introduced to be in compliance with the Release 12 specification of 3GPP TS 29.212. This feature is used to send detailed RAN and/or NAS release cause code information from the access network to PCRF. It requires that the NetLoc feature is also supported.

Important This feature can be enabled only when the NetLoc feature license is installed.

A new Diameter AVP "RAN-NAS-Release-Cause" will be included in the Charging-Rule-Report AVP and in CCR-T for bearer and session deletion events respectively, when the NetLoc-RAN-NAS-Cause supported feature is enabled. This AVP will indicate the cause code for the subscriber/bearer termination.

Configuring Supported Feature Netloc-RAN-NAS-Cause

The following configuration enables the supported feature "Netloc-RAN-NAS-Cause".

```
configure
    context  context_name
         ims-auth-service  service_name
              policy-control
                 diameter encode-supported-features netloc-ran-nas-cause

                   end
```

Notes:

- **netloc-ran-nas-cause**: Enables the Netloc-RAN-NAS-Cause feature. By default, this supported feature will be disabled.
- If the supported features "netloc-ran-nas-code" and "netloc" are enabled, then netloc-ran-nas-cause code will be sent to PCRF.

To disable this supported feature, use the following command:

```
[ default | no ] diameter encode-supported-features
```

Support ADC Rules over Gx Interface

In this release, P-GW will use Application Detection and Control (ADC) functionality over Gx as defined in the Release 11 specification of 3GPP standard.

ADC extension over Gx provides the functionality to notify PCRF about the start and stop of a specific protocol or a group of protocols, and provide the possibility to PCRF that with the knowledge of this information, change the QoS of the user when the usage of application is started and until it is finished.

The provision of ADC information is done through the ADC rule, the action initiated by PCRF is done through the PCC rule.

ADC rules are certain extensions to dynamic and predefined PCC rules in order to support specification, detection and reporting of an application flow. These rules are installed (modified/removed) by PCRF via CCA-I/CCA-U/RAR events. ADC rules can be either dynamic PCC or predefined PCC rules, and the existing attributes of dynamic and predefined rules will be applicable.

Dynamic PCC rule contains either traffic flow filters or Application ID. When Application ID is present, the rule is treated as ADC rule. Application ID is the name of the ruledef which is pre-defined in the boxer configuration. This ruledef contains application filters that define the application supported by P2P protocols.

PCEF will process and install ADC rules that are received from PCRF interface, and will detect the specified applications and report detection of application traffic to the PCRF. PCRF in turn controls the reporting of application traffic.

PCEF monitors the specified applications that are enabled by PCRF and generates Start/Stop events along with the Application ID. Such application detection is performed independent of the bearer on which the ADC PCC rule is bound to. For instance, if ADC rule is installed on a dedicated bearer whereas the ADC traffic is received on default bearer, application detection unit still reports the start event to PCRF.

Important ADC Rule support is a licensed-controlled feature. Contact your Cisco account representative for detailed information on specific licensing requirements.

In support of this feature, the following Diameter AVPs are newly added to the Charging-Rule-Definition AVP, which PCEF will receive from PCRF.

- TDF-Application-Identifier: It references the application detection filter which the PCC rule for application detection and control in the PCEF applies. The TDF-Application-Identifier AVP references also the application in the reporting to the PCRF.
- Redirect-Information: This indicates whether the detected application traffic should be redirected to another controlled address.
- Mute-Notification: This AVP is used to mute the notification to the PCRF of the detected application's start/stop for the specific ADC/PCC rule from the PCEF.

- Application Detection Information: If Mute-Notification AVP is not enclosed with charging rule report and APPLICATION_START/APPLICATION_STOP event trigger is enabled then PCEF will send Application-Detection-Information to PCRF corresponding TDF-Application-Identifier.

In addition, these two new event triggers "APPLICATION_START" and "APPLICATION_STOP" are generated for reporting purpose.

Limitations

The limitations for the ADC over Gx feature are:

- ADC does not support group of ruledefs.
- Registration of the duplicate application IDs are not supported.
- Readdress/Redirection for P2P flows will not be supported.
- Redirection happens only on transactions of GET/Response.
- Port based, IP Protocol based, and URL based applications are not supported.
- Pre-configured options (precedence, redirect-server-ip) for dynamic ADC rules are not supported.
- Simultaneous instances of an application for the same subscriber are not distinguished.
- Flow recovery is not supported for application flows.

Configuring ADC Rules over Gx

The following configuration enables ADC rules over Gx interface.

```
configure
   context  context_name
      ims-auth-service   service_name
         policy-control
            diameter encode-supported-features adc-rules
            end
```

Notes:

- The keyword "**adc-rules**" will be available only when the feature-specific license is configured.
- For ADC 6th bit of supported feature will be set.

To disable the support for ADC Rules over Gx, use the following command:

```
[ default | no ] diameter encode-supported-features
```

GoR Name Support in TDF-Application-Identifier

ASR 5500 supports dynamic rules to be installed with GoR name as TDF-Application-Identifier. When ADC rule is installed as a dynamic rule from PCRF, the TDF-Application-Identifier can include the GoR name pre-configured in the P-GW.

If the ADC feature is enabled, PCRF can send TDF-Application-Identifier as the name of GoR predefined in the P-GW configuration.

- When dynamic charging-rules with the Charging-Rule-Definition AVP are activated from PCRF, the PCRF can specify the GoR name configured in ECS as TDF-Application-Identifier.
- When dynamic charging-rules with the Charging-Rule-Definition AVP are activated, the PCRF can remove or modify the rule through the Charging-Rule-Definition using RAR. During rule activation or modification, the PCRF can add, modify or remove the charging-rule attributes of the rule.

The configuration changes for TDF-Application-Identifier from PCRF are listed below:

- A non-ADC dynamic rule can be changed to ADC dynamic rule by sending TDF-Application-Identifier AVP with relevant ruledef or GoR name.

  ADC dynamic rule cannot be changed to non-ADC dynamic rule.

- The following AVPs will be modified and applied when received from PCRF:
  - Precedence
  - Rating-Group/Service-Identifier/Sponsor-Identity (mandatory depending on the Reporting-Level)
  - Metering-Method
  - Online/Offline
  - QoS-Information
  - Monitoring-Key
  - Redirect-Information
- Dynamic route will be updated for all protocols of rules that are part of TDF-Application-Identifier GoR.
- Any change in dynamic rule priority or TDF-Application-Identifier value will lead to sending of APP-START and APP-STOP event notifications as new rule match. If an APP-START notification was sent already before rule modification, the corresponding APP-STOP notification will not be sent.
- Runtime deletion of associated GoR will take immediate effect and APP-STOP notification will not be sent if an APP-START was already sent. Addition of GoR at service level will need to have rules to be re-installed for the new addition to take effect for both dynamic and predefined ADC rules.

ADC Mute Customization

Earlier, 3GPP ADC over Gx did not support application MUTE status change. Once the application was muted, it was not possible to unmute it. From release 21.1, this feature introduces custom MUTE/UNMUTE functionality. ASR 5500 PCEF now supports customization to control reporting of the Application Detection Information CCRUs. For this, an AVP has been introduced with two possible values - custom MUTE and custom UNMUTE.

- A Gx message might contain both Standards based MUTE and the custom MUTE.
- Standards based MUTE is given preference over the custom MUTE/UNMUTE.
- A dynamic ADC rule can be installed and modified with a custom MUTE.
- Custom-Mute-Notification AVP can be sent by the PCRF in CCA-I and RAR.
- A dynamic ADC rule can be modified with a custom UNMUTE.
- On a custom MUTE for a given dynamic ADC rule, PCEF sends a single APPLICATION_START/ APPLICATION_STOP response for the entire application traffic rather the per flow APPLICATION_START /APPLICATION_STOP response.
- On a custom MUTE for a given dynamic ADC rule, if no APPLICATION_START has been sent prior to the custom MUTE then a single APPLICATION_START is sent on the next flow packet that hits the dynamic rule.
- On a custom MUTE for a given dynamic rule, the APPLICATION_START response is sent with the flow's 5-tuple information.

- On a custom MUTE for a given dynamic rule, the APPLICATION_START response is sent with TDF-Application-Instance-Identifier = 0.
- On a custom MUTE for a given dynamic rule, a single APPLICATION_STOP is sent when the last flow associated with the given dynamic rule is terminated. Such an APPLICATION_STOP will not contain 5-tuple information of the last flow and is sent with TDF-Application-Instance-Identifier = 0.
- On a custom UNMUTE for a given dynamic rule, APPLICATION STARTs response is matched with the given dynamic rule and then sent to all the forthcoming flows.
- There is no change in behavior for a custom UNMUTE, which has not been custom MUTED or standard MUTED before UNMUTING. APPLICATION_STARTs and APPLICATION_STOPs is continued to be sent per flow as before.
- On a custom UNMUTE, PCEF sends an APPLICATION_STOP each for all flows that terminate then onwards.
- A given dynamic rule is recovered in both SR and ICSR including the Custom MUTE/UNMUTE status. The APPLICATION_START status for a given dynamic rule is check-pointed and recovered. This ensures that an extra APPLICATION_START is not sent to the PCRF post recoveries.

Enhancement to the ADC Custom Mute/Unmute Functionality

Feature Information

Summary Data

Status	Modified Functionality
Introduced-In Release	21.1
Modified-In Release(s)	21.2
Applicable Product(s)	SAEGW
Applicable Platform(s)	ASR 5500
Default Setting	Disabled
Related CDETS ID(s)	CSCvd00699
Related Changes in This Release	Not Applicable
Related Documentation	Command Line Interface Reference SAEGW Administration Guide

Revision History

Important Revision history details are not provided for features introduced before release 21.2.

Revision Details	Release	Release Date
Modified in this release.	21.2	April 27, 2017

Feature Changes

The "ADC mute customization" feature introduced custom MUTE/UNMUTE functionality to control reporting of the Application Detection Information CCRUs. With the custom MUTE PCRF AVP, the PCRF informed P-GW when to disable/enable the ADC application notifications.

This feature enhances the "ADC mute customization" feature further and report the flow activities between custom mute and unmute events. P-GW learns the flow activities between custom mute events and then reports them to PCRF after the custom unmute event has occurred on the ADC rule. It minimizes the ADC application start and stop mechanism in standard ADC mute and unmute case.

A new CLI command has been implemented at the rulebase, which when configured, reports ADC application start and stop notifications only once per rule. This helps in reducing messaging flows towards the PCRF.

Limitations

Following are the limitations of this feature:

- P-GW stores maximum of 12 learned flows per ADC rule. Once the limit 12 has been reached, P-GW forgets the oldest flow and learns about the latest flow. Once P-GW receives the custom unmute event, it notifies the PCRF about the learned notifications. P-GW sends application stop notification, if the application start notification for the flow is sent.
- Flow information stored for sending the application start notifications to the PCRF after the event of the custom unmute is not recovered.
- On LTE to WiFi handover, the values received from the PCRF for custom mute or custom unmute per ADC dynamic rule gets applied in the new RAT. If there is no value received in the handover context, the previous values before the RAT change are retained for all the ADC dynamic rules which are present.
- If the CLI command **adc notify** is enabled, then the single ADC application start and stop notification is notified to the PCRF. If there are multiple flows which match the same ADC dynamic rule, only one application start and stop notification is sent to the PCRF.
- This feature is implemented only for the dynamic rules.

How it Works

Following is the sequence of events that occur when P-GW receives packet and ADC rule event occurs from PCRF:

1. Packet reaches the ECS rule matching engine.
2. The rule matching engine checks if the ADC dynamic rule is matched. It also checks if the custom mute is applied through the PCRF or rulebase level CLI. A single application start notification is sent, if not sent earlier.
3. For all the subsequent flows matching the same ADC rule, application start notification is stored. These notifications are sent in the CCRU after the custom unmute event is received.

Following are some important points:

- The values received from the PCRF has the highest priority. Hence, standard mute has the highest priority than custom-mute/custom-unmute. The CLI *adc notify once* has the least priority.
- If the CLI **adc notify once** is configured at the rulebase, the converse **no adc notify** does not have any impact. To converse the CLI impact, do either of the following tasks:

- Switch the rulebase in which the CLI **adc notify once** is not configured.
- Send the "custom unmute" for that particular dynamic rule.

Configuring the ADC Notifications

The new CLI command, **adc notify**, has been added to the active charging service mode.

When this CLI is configured, a single application start or application stop notification for the ADC flow matching per rule is sent to the PCRF. If this CLI is configured and the PCRF sends the custom mute notification, then the PCRF notification takes precedence over the standard behavior for reporting the notification.

The default value of this keyword is false. If this CLI is not configured, then no action is taken on sending the ADC notifications.

To enable or disable the feature, enter the following commands:

```
configure
  active-charging service <service_name>
    rulebase <rulebase_name>
      [no] adc notify [once]
      end
```

For configuring single notification use the following command:

```
adc notify once
```

Notes:

- **no:** Disables the ADC notifications and ADC notifications are sent as per default behavior.
- **adc:** Configures the ADC notifications.
- **notify:** Configures the application notification. If this keyword is not configured, ADC notifications are sent as per default behavior.
- **once:** Configures the application notification only once. PCRF takes the priority.

Support for TAI and ECGI Change Reporting

This section describes the overview and implementation of TAI and ECGI Change Reporting feature.

This section discusses the following topics for this feature:

- Feature Description, on page 157
- How it Works, on page 158
- Monitoring and Troubleshooting the TAI and ECGI Change Reporting Feature, on page 159

Feature Description

For activating User Location Reporting for a UE over Gx, PCRF sends RAR/CCA with the "USER_LOCATION_CHANGE (13)" event trigger. On receiving this event trigger, P-GW typically sends

Change Reporting Action (CRA) Information Element (IE) with "Start Reporting" towards MME to enable the Location-Change reporting for the UE in MME.

In the current architecture, the "USER_LOCATION_CHANGE (13)" trigger is used to report the changes in User Location Information (ULI), Tracking Area Identity (TAI) and E-UTRAN Cell Global Identifier (ECGI). In release 19.4 and beyond, separate event triggers TAI_CHANGE (26) and ECGI_CHANGE (27) are supported for reporting the changes in TAI and ECGI correspondingly. CLI changes are done to display the new event triggers in show configuration commands.

Important For TAI reporting to work, the **diameter map usage-report** CLI command must be configured in Policy Control configuration mode to use the value 33.

PCRF subscribes to the CRA event for reporting change of TAI and ECGI. P-GW sends event trigger in CCR-U only if it is subscribed by PCRF. When PCRF installs the event trigger for ECGI Change and/or TAI change, any change in ECGI and TAI (based on installed triggers) is reported.

The TAI and ECGI Change Reporting feature complies with 3GPP TS 29.212 v9.7.0. This feature is supported on Gx interface so that UE can be tracked on ECGI/TAI change and reported to PCRF. For more information on the User Location Information Reporting feature, see the administration guide for the product that you are deploying.

In releases prior to 19.3, the CRA event included in Create Session Response (CSRsp) for reporting location change was always set to START_REPORTING_ECGI (4).

In release 19.4 and beyond, the CRA value varies based on the event triggers received from PCRF.

Change Reporting Support Indication (CRSI) and ULI are also supported in Bearer Resource Command.

P-GW sends the ULI received in Delete Bearer Command from MME to PCRF when the corresponding Delete Bearer Response is received. When the ULI is included in both Delete Bearer Command and Delete Bearer Response, the ULI in Delete Bearer Response is sent to the PCRF. In the absence of ULI in Delete Bearer Response, then the ULI received in Delete Bearer Command is sent to PCRF.

Relationships to Other Features

This feature has a dependency on USAGE_REPORT value of Event-Trigger AVP. This feature works only when the value of USAGE_REPORT is set to 33. This can be achieved using the **diameter map usage-report** CLI command in Policy Control configuration mode.

How it Works

P-GW sends Event Trigger value based on the event trigger detected by P-GW in CCR-U. P-GW sends Event Trigger and ULI Type in CCR-U to PCRF as per the following table.

Event Trigger from PCRF	CRA Value	Event Detected at P-GW	What to Inform PCRF
ULI_CHANGE	6	TAI_CHANGE or ECGI_CHANGE	Event Trigger: ULI_CHANGE ULI Type: TAI + ECGI
TAI_CHANGE	3	TAI_CHANGE	Event Trigger: TAI_CHANGE ULI Type: TAI

Event Trigger from PCRF	CRA Value	Event Detected at P-GW	What to Inform PCRF
ECGI_CHANGE	4	ECGI_CHANGE	Event Trigger: ECGI_CHANGE ULI Type: ECGI
ULI_CHANGE + TAI_CHANGE	6	TAI_CHANGE	Event Trigger: ULI_CHANGE+ TAI_CHANGE ULI Type: TAI+ECGI
ULI_CHANGE + ECGI_CHANGE	6	ECGI_CHANGE	Event Trigger: ULI_CHANGE + ECGI_CHANGE ULI Type: TAI+ECGI
ULI_CHANGE + TAI_CHANGE + ECGI_CHANGE	6	TAI/ECGI has changed	Event Trigger: ULI_CHANGE + TAI/ECGI CHANGE ULI_Type: TAI+ECGI
TAI_CHANGE + ECGI_CHANGE	6	TAI/ECGI has changed	Event Trigger: TAI_CHANGE/ECGI_CHANGE ULI_Type: TAI+ECGI
For combinations not specifically mentioned above	6		Event Trigger: ULI_CHANGE ULI_Type: TAI+ECGI

Limitations

TAI and ECGI Change Reporting feature is supported only when ***diameter map usage-report*** CLI command is configured as 33.

Monitoring and Troubleshooting the TAI and ECGI Change Reporting Feature

This section provides information regarding show commands and/or their outputs in support of the TAI and ECGI Change Reporting feature.

show ims-authorization sessions full all

The following fields are added to the output of this show command in support of this feature:

- TAI-Change - Displays this event trigger when TAI has changed for a subscriber session.
- ECGI-Change - Displays this event trigger when ECGI has changed for a subscriber session.

show ims-authorization service statistics all

The following statistics are added to the output of this show command in support of this feature:

- TAI Change - Displays the total number of times P-GW has reported TAI_CHANGE (26) event trigger to PCRF.
- ECGI Change - Displays the total number of times P-GW has reported ECGI_CHANGE (27) event trigger to PCRF.

Location Based Local-Policy Rule Enforcement

This section describes the overview and implementation of Location-based Local-Policy (LP) Rule Enforcement feature.

This section discusses the following topics for this feature:

- Feature Description, on page 160
- How it Works, on page 161
- Configuring Location Based Local Policy Rule Enforcement Feature, on page 162
- Monitoring and Troubleshooting the Location Based LP Rule Enforcement Feature, on page 164

Feature Description

This feature is introduced to activate different predefined rules for different E-UTRAN Cell Global Identifiers (ECGIs) when the subscriber is connected to a corporate APN. The subscriber has to explicitly bring down the connection with the corporate APN and re-establish session with Internet APN when out of the company area. It is assumed that corporate APN does not use PCRF and use only Local-Policy. In this case, all calls matching the APN is directed to the Local-Policy.

Important For this feature to work, the license to activate Local-Policy must be configured. For more information on the licensing requirements, contact your local Cisco account representative.

To activate different predefined rules for ECGI, Local-Policy configurations are enhanced to support:

- Configuration and validation of a set of ECGIs
- Installation of ECGI_CHANGE event trigger through Change Reporting Action (CRA) event
- Detection of ECGI_CHANGE event

This feature supports the following actions to be applied based on the ECGI match with Local-Policy ruledef condition:

- Enable a redirect rule on ECGI_CHANGE event notification when the ECGI belongs to a certain group
- Enable a wild card rule for any other ECGIs

Relationships to Other Features

This feature has a dependency on TAI and ECGI Change Reporting feature, which provides a framework to report ECGI-Change from session manager module to IMSA/Local-Policy module.

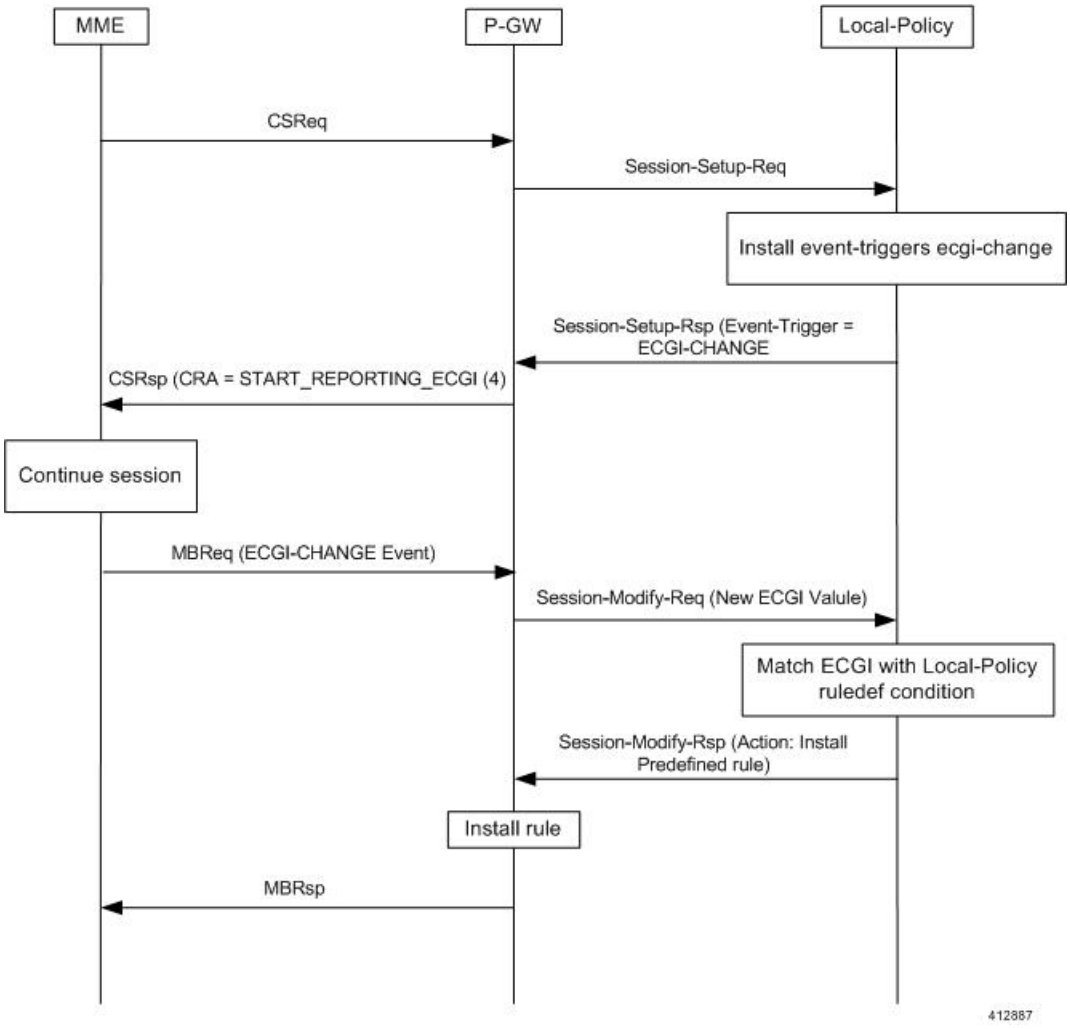
How it Works

This section describes how the Local Policy Rule selection and enforcement happens based on ECGI-CHANGE event trigger.

Flows

The following figure describes how the ECGI-CHANGE event is being handled in Local-Policy, MME and P-GW.

Figure 14: ECGI-CHANGE Event Handling



When a new call is established the ECGI-CHANGE event trigger is sent from Local-Policy. P-GW requests the MME for ECGI reporting by sending CRA of 4 in Create Session Response (CSRsp). MME informs the P-GW of ECGI Change through Change Notification request/Modify Bearer Request (MBReq). Local-Policy configuration at P-GW will handle the ECGI-CHANGE event and take appropriate action based on the ECGI group to which the new ECGI belongs. One action could be to activate a certain redirect rule when ECGI belongs to a certain group, and other action could be to enable a wildcard rule for any other ECGI.

Limitations

This section identifies the known limitations of this feature.

- ECGI Change detection and triggering is a pre-requisite for this feature.
- This feature is supported for Local-Policy-only (lp-only) mode wherein, all requests and responses within a particular APN directly go to Local-Policy without contacting PCRF. That is, this feature does not work in Local-Policy fallback mode and dual mode wherein both PCRF and Local-Policy co-exist.

Configuring Location Based Local Policy Rule Enforcement Feature

This section provides the configuration of parameters within Local-Policy to enable rule enforcement based on ECGI-Change event notification.

Configuring ECGI Change Trigger

Use the following configuration to install ECGI-Change trigger from local-policy.

```
configure
   local-policy-service service_name
      actiondef actiondef_name
         action priority priority event-triggers ecgi-change
         exit
      eventbase default
         rule priority priority event new-call ruledef ruledef_name actiondef
 actiondef_name [ continue ]
         end
```

Notes:

- **priority** *priority*: Specifies a priority for the specified action. *priority* must be unique and an integer from 1 to 2048.
- **ecgi-change**: This keyword specifies to install ECGI-CHANGE event trigger. If enabled, ECGI-CHANGE event trigger is sent from local-policy.
- This CLI command is configured in local-policy if operator wants to enable ECGI-Change notification in MME by sending a CRA value.

Applying Rules for ECGI-Change Event

Use the following configuration to enable ECGI Change detection and take specific action for ECGI-CHANGE event reported by MME.

```
configure
   local-policy-service service_name
      eventbase eventbase_name
         rule priority priority event ecgi-change ruledef ruledef_name
actiondef actiondef_name [ continue ]
         end
```

Notes:

- **priority** *priority*: Specifies a priority for the specified rule. *priority* must be unique and an integer from 1 to 2048.

- **ruledef** *ruledef_name*: Associates the rule with a specific ruledef. *ruledef_name* must be an existing ruledef within this local QoS policy service.
- **actiondef** *actiondef_name*: Associates the rule with a specific actiondef. *actiondef_name* must be an existing actiondef within this local QoS policy service expressed as an alphanumeric string of 1 through 63 characters.
- **ecgi-change**: Enables a new event to detect ECGI-CHANGE and applies specific action for the ECGI-CHANGE event as defined in actiondef configuration.
- **continue**: Subsequent rules are also matched; otherwise, rule evaluation is terminated on first match.

Enforcing Local Policy Rule based on ECGI Value

Use the following configuration to apply rules based on the ECGI value received in ECGI-Change event notification by MME.

```
configure
   local-policy-service service_name
      ruledef ruledef_name
         condition priority priority ecgi mcc mcc_num mnc mnc_num eci { eq |
ge | gt | le | lt | match | ne | nomatch } regex | string_value | int_value |
 set }
         end
```

Notes:

- **priority** *priority*: Specifies a priority for the specified condition. *priority* must be unique and an integer from 1 to 2048.
- **ecgi mcc** *mcc_num* **mnc** *mnc_num* **eci**: Configures ECGI with values for MCC, MNC and ECI.
  - **mcc** *mcc_num* : MCC is a three digit number between 001 to 999. It is a string of size 3 to 3.
  - **mnc** *mnc_num* : MNC is a two/three digit number between 01 to 999. It is a string of size 2 to 3.
  - **eci**: ECI is a hexadecimal number between 0x1 to 0xffffffff. It is a string of size 1 to 7.
- This CLI command is configured in local-policy if operator wants to take specific action based on certain ECGI value received in ECGI-Change event notification by MME.

Verifying the Location Based LP Rule Enforcement Configuration

Use the following command to verify the configuration of this feature.

```
show configuration context
```

Important This feature is supported for Local-Policy-only mode wherein, all requests and responses within a particular APN directly go to Local-Policy without contacting PCRF.

Here is an example configuration for this feature.

```
configure
   context source
```

```
      apn corporate-apn
         ims-auth-service LocalPolicy_1
      exit
   exit
end

configure
   local-policy-service LocalPolicy_1
      ruledef any-imsi
         condition priority 1 imsi match *
      exit
      ruledef ecgi-group
         condition priority 1 ecgi mcc 123 mnc 456 eci eq ffff
      exit
      actiondef ecgi-trigger
         action priority 1 event-triggers ecgi-change
      exit
      actiondef ecgi-redirect-rule
         action priority 1 activate-rule namerule-1
      exit
      eventbase default
        rule priority 1 event new-call ruledef any-imsi actiondef ecgi-trigger

         rule priority 2 event ecgi-change ruledef ecgi-group actiondef
ecgi-redirect-rule
         rule priority 3 event location-change ruledef ecgi-group actiondef
 ecgi-redirect-rule
      exit
   exit
end
```

Monitoring and Troubleshooting the Location Based LP Rule Enforcement Feature

This section provides information regarding show commands and/or their outputs in support of the Location Based Local Policy Rule Enforcement feature.

Use the following CLI commands to troubleshoot if any issue is encountered with this feature.

show configuration context

logging filter active facility local-policy level debug

show local-policy statistics

show active-charging sessions full

show local-policy statistics summary

The following statistics are added to the output of this show command to support the ECGI-CHANGE event trigger installation:

- Event Statistics:
  - ECGI Change - Displays the number of ECGI-CHANGE event triggers that has been received by Local-Policy.

- Variable Matching Statistics
  - ECGI - Displays the number of times the ECGI is matched and the specific action is applied based on the event.

Gx Support for GTP based S2a/S2b

In releases prior to 18, for WiFi integration in P-GW, Gx support was already available for GTP based S2a/S2, but the implementation was specific to a particular customer.

In 18 and later releases, the Gx support for GTP based S2a/S2 interface is extended to all customers. This implementation is in compliance with standard Rel.8 Non-3GPP specification part of 29.212, along with C3-101419 C3-110338 C3-110225 C3-120852 C3-130321 C3-131222 CRs from Rel.10/Rel.11.

As part of this enhancement, the following changes are introduced:

- AVP support for TWAN ID is provided
- TWAN-ID is added to r8-gx-standard dictionary

Gx-based Virtual APN Selection

This section describes the overview and implementation of Gx based Vitrual APN Selection feature.

This section discusses the following topics for this feature:

- Feature Description, on page 165
- Configuring Gx based Virtual APN Selection Feature , on page 166
- Monitoring and Troubleshooting the Gx based Virtual APN Selection, on page 166

Feature Description

Overview

The current implementation supports Virtual APN (VAPN) Selection through RADIUS or local configuration. In Release 19, ASR 5500 uses PCRF and Gx interface for Virtual APN selection to achieve signaling reduction.

A new supported feature "**virtual-apn**" with feature bit set to 4 is added to the IMSA configuration. This configuration enables Gx based Virtual APN Selection feature for a given IMS authorization service. When this configuration is enabled at P-GW/GGSN, then P-GW/GGSN advertises this feature to PCRF through the Supported-Features AVP in CCR-I. When the VAPN is selected, then the PCRF rejects the CCR-I message with the Experimental-Result-Code AVP set to 5999 (DIAMETER_GX_APN_CHANGE), and sends a new APN through the Called-Station-Id AVP in CCA-I message. The existing call is then disconnected and reestablished with the new virtual APN. Note that the Experimental Result Code 5999 will have the Cisco Vendor ID.

Important Enabling this feature might have CPU impact (depending on the number of calls using this feature).

License Requirements

This feature requires a valid license to be installed prior to configuring this feature. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Limitations

The following are the limitations of this feature:

- Virtual APN supported feature negotiation, Experimental Result Code (5999), Called-Station-Id AVP should be received to establish the call with new virtual APN. When any one of conditions is not met then the call will be terminated.
- Failure-handling will not be taken into account for 5999 result-code when received in the CCA-I message.
- When the Experimental Result Code 5999 is received in the CCA-U then failure-handling action will be taken.
- If the Called-Station-Id AVP is received in CCA-U or CCA-T, then the AVP will be ignored.
- If virtual-apn is received in local-policy initiated initial message then the call will be terminated.
- When PCRF repeatedly sends the same virtual-apn, then the call will be terminated.

Configuring Gx based Virtual APN Selection Feature

The following section provides the configuration commands to enable the Gx based Virtual APN Selection.

```
configure
    context context_name
        ims-auth-service service_name
            policy-control
                diameter encode-supported-features virtual-apn
                end
```

Notes:

- **virtual-apn**: This keyword enables configuration of Gx-based Virtual APN Selection feature. By default, this feature is disabled.
- This keyword is license dependent. For more information, contact your Cisco account representative.

Verifying the Gx based Virtual APN Configuration

Use the following command in Exec mode to display whether the Gx based Virtual APN Selection feature is configured as part of the Supported-Features AVP.

```
show ims-authorization sessions full all
```

The "Negotiated Supported Features" field in this show command output displays the configuration status. This supported feature is displayed only when the feature license is configured.

Monitoring and Troubleshooting the Gx based Virtual APN Selection

This section provides information regarding show commands and/or their outputs in support of this feature.

show ims-authorization policy-control statistics

The following field has been added to the output of this show command to track the number of times the PCRF sends the Diameter Experimental Result Code (5999) when a new virtual APN is selected.

- **Gx APN Change**

For descriptions of this statistics, see the *Statistics and Counters Reference* guide.

Debugging Statistics

Use the following command to debug the Gx based Virtual APN calls.

```
show session subsystem facility sessmgr debug-info
```

This command displays the detailed statistics associated with the Gx-based VAPN feature. For example, number of Gx VAPN received, number of AAAMGR/SGX/DHCP messages after enabling Gx VAPN, and Gx VAPN calls setup time.

Bulk Statistics for Gx based Virtual APN Selection Feature

IMSA Schema

The following new bulk statistic variable is added to the IMSA schema to track the number of times the PCRF sends the Diameter Experimental Result Code (5999) when a new virtual APN is selected.

- dpca-expres-gx-apn-change

For descriptions of this variable, see the *Statistics and Counters Reference* guide.

System Schema

The following new disconnect reason is added to the System schema to track the number of times a P-GW/GGSN/SAEGW session was disconnected due to validation failure of virtual APN received from PCRF.

- gx-vapn-selection-failed (618)

For descriptions of this variable, see the *Statistics and Counters Reference* guide.

Graceful Handling of RAR from Different Peers

In StarOS Gx architecture, every Diameter session is associated with a Primary and a Secondary peer when host select is configured at the IMSA service. The behavior for processing RAR prior to release 20 is as follows:

- If the RAR is received from the Primary peer for the session, the RAR is responded using the Primary peer connection.
- If the RAR is received from a Secondary peer for the session, host-switch takes effect. This results in the RAA (and any further session signaling) happening via the Secondary peer.
- If the RAR is received via a third peer which is neither the Primary nor the Secondary peer for the session, the RAR is dropped.

In certain networks where PCRF and PCEF are connected through multiple DRAs the PCRF may select the DRA in a round-robin fashion and the RAR for a session may come from a peer which is neither Primary nor Secondary. In order to handle such a scenario, the ability to respond to the RAR received from a non-primary and non-secondary peer was added. In this case, the RAR is answered via the peer from which RAR was received. However any future signaling for the session will still occur via the previously communicating peer. If the RAR is received via the secondary peer, the host-switch occurs and the behavior remains unchanged. In order to be able to process the RAR from a third peer, that peer must be configured in the Diameter endpoint configuration. Further, this issue is seen only when host select is configured at IMSA service. When the host selection happens at endpoint level, this issue is not seen.

Assume there are three DRAs and they are configured as shown in the sample configuration below:

```
configure
   context test
      diameter endpoint Gx
         ...
         peer DRA1 realm realmName address 192.168.23.3
         peer DRA2 realm realmName address 192.168.23.3 port 3869
         peer DRA3 realm realmName address 192.168.23.3 port 3870
         exit
      ims-auth-service imsa-Gx
         policy-control
            diameter host-select row-precedence 1 table 1 host DRA1
secondary host DRA2
end
```

Without the feature, when RAR is received from DRA3, it is rejected. With the feature enabled, RAR from DRA3 is responded via DRA3 only and Peer switch will not occur in this case and subsequent messaging will be sent through DRA1 or DRA2 if any prior peer switch had happened.

Limitations

This section identifies the limitations for this feature.

- RAR will be rejected when received from different origin host.
- RAR will be rejected when received from a DRA not configured in Diameter endpoint.

NetLoc Feature Enhancement

This feature adds compliance with 3GPP standard R13 version to the existing NetLoc feature functionality.

Feature Description

Important This is a license controlled feature. Netloc feature license key is required to be enabled. Contact your Cisco account representative for information on how to obtain a license.

This feature adds compliance with 3GPP standard R13 version to the existing NetLoc feature functionality. Using this NetLoc feature, the IMS network can retrieve location information of the UE from the access or LTE network. This enhances the location related functionality and charging based on the location information.

This feature introduces the following behavior changes:

- Assuming that NetLoc feature is enabled on chassis and Access Network Information (ANI-45) Event trigger is installed, following behavior changes have been introduced:

Table 9: Gx Interface Behavior Change Towards PCRF

PCRF Gx Interface Interaction	Access Side Interaction	ULI & MS TZ Behavior Before 21.1 Release(Standard Gx-R8/Custom15 (AT&T))	ULI & MS TZ Behavior Change(Standard Gx-R8/Custom15 (AT&T))
RAI AVP with '0 - ULI' is received in the charging rule install request.	Create Bearer Response is received with **only New ULI** parameter.	Create Bearer Response is received with **only New ULI** parameter.	No change in the behavior.
RAI AVP with '0 - ULI' is received in the charging rule install request.	Create Bearer Response is received with **No ULI** parameter.	Old ULI parameter is sent towards the PCRF in the CCR-U message.	PLMN-id in 3GPP-SGSN-MCC-MNC AVP is sent towards the PCRF.
RAI AVP with '0 - ULI' is received in the charging rule modify request.	Update Bearer Response is received with **only New ULI** parameter.	New ULI parameter is sent towards the PCRF in the CCR-U message.	No change in the behavior.
RAI AVP with '0 - ULI' is received in the charging rule Modify request.	Update Bearer Response is received with **No ULI** parameter.	Old ULI parameter is sent towards the PCRF in the CCR-U message.	PLMN-id in 3GPP-SGSN-MCC-MNC AVP is sent towards the PCRF.
RAI AVP with '0 - ULI' is received in the charging rule modify request.	Delete Bearer Response is received with **only New ULI** parameter and No MS TZ parameter.	New ULI and old MS TZ parameters are sent towards the PCRF in the CCR-U message.	Only New ULI is sent towards the PCRF in the CCR-U message.
RAI AVP with '0 - ULI' is received in the charging rule Modify request.	Delete Bearer Response is received with **No ULI** parameter and No MS TZ parameter.	Old ULI and old MS TZ parameters are sent towards the PCRF in the CCR-U message.	PLMN-id in the 3GPP-SGSN-MCC-MNC AVP is sent towards the PCRF.
RAI AVP with '1 -MSTZ' is received in the charging rule install request.	Create Bearer Response is received with **only new MS TZ** parameter.	New MS TZ parameter is sent towards the PCRF in the CCR-U message.	No change in the behavior.
RAI AVP with '1 -MSTZ' is received in the charging rule install request.	Create Bearer Response is received with **No MS TZ** parameter.	Old MS TZ parameter is sent towards the PCRF in the CCR-U message.	No change in the behavior.

PCRF Gx Interface Interaction	Access Side Interaction	ULI & MS TZ Behavior Before 21.1 Release(Standard Gx-R8/Custom15 (AT&T))	ULI & MS TZ Behavior Change(Standard Gx-R8/Custom15 (AT&T))
RAI AVP with '1 -MSTZ' is received in the charging rule modify request.	Update Bearer Response is received with **only New MS TZ** parameter.	New MS TZ parameter is sent towards the PCRF in the CCR-U message.	No change in the behavior.
RAI AVP with '1 -MSTZ' is received in the charging rule Modify request.	Update Bearer Response is received with **No MS TZ** parameter.	Old MS TZ parameter is sent towards the PCRF in the CCR-U message.	No change in the behavior.
RAI AVP with '1 -MSTZ' is received in the charging rule modify request.	Delete Bearer Response is received with **only New MS TZ** parameter.	Old ULI and New MS TZ parameters are sent towards the PCRF in the CCR-U message.	Only New MS TZ is sent towards the PCRF in the CCR-U message.
RAI AVP with '1 -MSTZ' is received in the charging rule Modify request.	Delete Bearer Response is received with **No MS TZ** parameter.	New ULI and old MS TZ parameters are sent towards the PCRF in the CCR-U message.	Only old MS TZ is sent towards the PCRF.
Nothing is received.	Delete Session Request is received with New ULI and New MS TZ parameters.	New ULI and New MS TZ parameters are sent towards the PCRF in the CCR-T message.	No change in the behavior.
Nothing is received.	Delete Session Request is received with New ULI and No MS TZ parameter.	New ULI and Old MS TZ parameters are sent towards the PCRF in the CCR-T message.	No change in the behavior.
Nothing is received.	Delete Session Request is received with No ULI and No MS TZ parameter.	Old ULI and Old MS TZ parameters are sent towards the PCRF in the CCR-T message.	No change in the behavior.

Important ULI and ULI timestamp is considered as paired. If the ULI timestamp is forwarded, it is forwarded and received with the ULI. If the ULI is received and the ULI timestamp is not received, then that P-GW does not forward the old timestamp.

- Inclusion of AVP support of NETLOC-ACCESS-NOT-SUPPORTED on Gx interface. This inclusion of AVP is based on the below conditions:
  - RAT type is other than E-UTRAN, UTRAN, WCDMA, GPRS, GERAN, and W-LAN
  - IP CAN type is other than 3GPP EPS, GPRS, and non 3GPP EPS

- Re-Auth-Request is received with Required-Access-Info AVP.
- NetLoc feature is enabled on the chassis.
- Event-Trigger ACCESS_NETWORK_INFO_REPORT (45) is installed.

Before Release 21.1 Behavior (Standard Gx-R8/Custom15(AT&T))	New Behavior(Standard Gx-R8/Custom15(AT&T))
Earlier, if IP-CAN type or RAT type was not support NETLOC, P-GW(PCEF) ignored RAI received from the PCRF.	New AVP NetLoc-Access-Support has been added in the Re-Auth-Answer message in the R8-Gx-standard and the Custom15 Gx Dictionary.

- ***Table 10: Behavior Change Regarding LastUserLocationInformation AVP and LastMSTimeZone AVP***

P-GW CDR Behavior	Post 21.1 Release, Behavior in Custom 35/Custom 24/Custom 48 Dictionaries	Custom52 Dictionary (standard compliance new dictionary)/ Custom 35 Dictionary (Customer Specific)
ULI is received in Delete Bearer Command/Delete Bearer Request /Delete Session Request.	ULI was not part of P-GW CDR generation.	ULI is recorded as **LastUserLocationInformation** AVP in the P-GW CDR generation. (AVP is not controlled using the CLI command.)
MS TZ is received in the Delete Bearer Command/Delete Bearer Request /Delete Session Request.	MS TZ was not part of P-GW CDR generation.	MS TZ is recorded as **LastMSTimeZone** AVP in the P-GW CDR generation. CDR is released as Normal Release. MS TZ is not detected in this case as full trigger and does not release extra CDR with MS TZ changes cause. AVP is not controlled using the CLI command.

S-GW CDR behavior	Post 21.1 Release behavior in Custom 35/Custom 24 Dictionary	Custom24 Dictionary (standard dictionary)/ Custom 35 Dictionary (AT&T)
ULI is received in Delete Bearer Command/Delete Bearer Request /Delete Session Request.	ULI was not part of CDR generation.	ULI is Recorded as **LastUserLocationInformation** AVP in the S-GW CDR generation. The attribute is controlled using a CLI command.

MS TZ is received in Delete Bearer Command/Delete Bearer Request /Delete Session Request.	MS TZ was not part of CDR generation.	MS TZ is Recorded as **LastMSTimeZone** AVP in S-GW CDR generation. The attribute is controlled using a CLI command. CDR is released as Normal Release. MS TZ is not detected in this case as full trigger and does not release extra CDR with MS TZ changes cause.

Limitations

1. This feature enhancement is applicable only for S-GW, P-GW, and SAEGW. For GGSN ad SGSN, there is no change in the behavior of the NetLoc feature.
2. The attributes **Last-MS-Timezone** and **Last ULI attributes** have been added in the dictionaries custom24 and custom35 for S-GW CDR generation only.
3. The keywords **last-ms-timezone** and **last-uli** added to the CLI command **gtpp attribute** are applicable and limited to only S-GW CDR generation.
4. **Last-MS-Timezone** and **Last ULI attributes** added in dictionary custom35 (customer specific dictionary) and custom52 (3GPP R13 standard compliance) are applicable and limited to P-GW CDR generation only. These attributes are not CLI controlled.

Command Changes

gtpp-attribute

This CLI command allows the specification of the optional attributes to be present in the Call Detail Records (CDRs) that the GPRS/PDN/UMTS access gateway generates. It also defines that how the information is presented in CDRs by encoding the attribute field values. The keywords **last-ms-timezone** and **last-uli** have been added to this CLI command to control attribute while CDR generation.

Important The keywords added are applicable only for S-GW CDR. They are not applicable for P-GW CDR.

```
configure
   context <context_name>
      gtpp group group_name
        gtpp attribute { last-ms-timezone | last-uli | .. }
        [no | default ] gtpp attribute { last-ms-timezone | last-uli |
.. }
    end
```

Notes:

- **no:** Removes the configured GTPP attributes from the CDRs.
- **default:** Sets the default GTPP attributes in the generated CDRs. It also sets the default presentation of attribute values in generated CDRs.

- **last-ms-timezone:** Sets the "Last MS-Timezone" in the CDR field. This option would be disabled when the default option is used.
- **last-uli:** Sets the "Last ULI" in the CDR field. This option would be disabled when the default option is used.

Performance Indicator Changes

show configuration

This command has been modified to display the following output:

- Last-MS-Timezone present
- Last-User Location Information present

show gtpp group name *group_name*

This command has been modified to display the following output:

```
     Last-MS-Timezone present: yes
     Last-User Location Information present:
yes
```

RAN-NAS Cause Code Feature Enhancement

This chapter describes the RAN-NAS Cause Code Feature Enhancement.

Feature Description

Important This is a license controlled feature. You must enable the existing license of NPLI. Contact your Cisco account representative for information on how to obtain a license.

This feature introduces support for 3GPP RAN/NAS cause code IE for "Failed Create Bearer Response", "Failed Updated Bearer Response", and "Delete Bearer Response" at the Gx interface, the P-GW, and S-GW CDRs. This will enable the operator to get detailed RAN/NAS release cause code information from the access network. RAN/NAS cause can be received from the access side in either of the following messages:

- Failed Create Bearer Response
- Failed Update Bearer Response
- Delete Session Request
- Delete Bearer Response
- Delete Bearer Command

This support of 3GPP Release 12 RAN/NAS cause IE on the S4, S11, S5, and S8 interfaces exists for "Delete Session Request" and "Delete Bearer" command through private extension as well as Standard IE for customer specific dictionaries Gx- dpca-custom15 and Gz-Custom35.

However, RAN/NAS cause received in the "ERAB creation Failure", "ERAB modification Failure", and "ERAB release indication" messages were not processed at the S-GW and P-GW. Hence, it was also not forwarded to the PCRF by P-GW neither populated in the P-GW and S-GW CDRs. With this feature enhancement, support has been added to process the RAN/NAS cause codes at the S-GW (S4,S11 interface) and P-GW (S5,S8 interface) for the "Create bearer response", "Update bearer response", and "Delete bearer response". Also, RAN/NAS cause codes will be forwarded to the PCRF by the P-GW and will be populated in the P-GW and S-GW CDRs.

There is no requirement to add the support for the 3GPP Release 12 RAN/NAS cause IE received in the private extension for "Create Bearer Response", "Update Bearer Response", and "Delete Bearer Response". Private extension support for 3GPP Release 12 cause code IE in "Delete Session Request" and "Delete Bearer Command" will continue to be supported.

This feature enhancement introduces the following RAN/NAS cause IE behavior changes at the Gx interface for dpca-custom15 dictionary and at Gz interface for custom35 dictionary.

Table 11: Gx Interface Requirements for RAN/NAS Cause

Message	GTP Cause	Gx Message Carrying RAN-NAS Cause Information
Create Bearer Response	Accepted	RAN/NAS cause is not expected as per 29.274 Table 7.2.4-2. So if it is received, it is ignored and is not forwarded to the PCRF.
	Temporarily rejected due to HO in progress.	RAN/NAS cause with this GTP cause is not applicable as per 29.274 Table C.4. So if received it is ignored and is not forwarded to the PCRF.
	Other GTP Causes	CCR-U
Update Bearer Response	Accepted	RAN/NAS cause is not expected as per 29.274 Table 7.2.16-2. So if it is received, it is ignored and is not forwarded to the PCRF.
	No Resources	CCR-U
	Available	**Important** If the UE-initiated (MBC) bearer modification fails with the GTP cause "NO RESOURCES AVAILABLE", then P-GW deletes the entire PDN session. In this case, RAN-NAS cause information is forwarded as part of the CCR-T message.
	Context Not Found	If the update bearer response is received with the message level cause as "CONTEXT NOT FOUND", which leads to the PDN deletion, then the RAN-NAS cause information is forwarded as part of the CCR-T message.
	Temporarily rejected due to HO in progress.	RAN/NAS cause with this GTP cause is not applicable as per 29.274 Table C.4. So if this cause is received, it is ignored and is not forwarded to the PCRF.
	Other GTP Causes	CCR-U

Message	GTP Cause	Gx Message Carrying RAN-NAS Cause Information
Delete Bearer Response	Temporarily rejected due to HO in progress	RAN/NAS cause with this GTP cause is not applicable as per 29.274 Table C.4. So if this cause is received, it is ignored and is not forwarded to the PCRF. **Important** As per existing design of S-GW, if "Delete Bearer Response" is received with GTP cause "Temporarily rejected due to handover/ TAU/ RAU procedure in progress" it changes GTP cause to "Request Accepted" and forwards it to the P-GW. In this case, if RAN/NAS cause is received in the "Delete Bearer Response", S-GW will forward it to the P-GW. And at the P-GW since "Delete Bearer Response" is received with the GTP cause "Request Accepted" hence RAN/NAS cause is forwarded to the PCRF and populated in the P-GW CDR. This behavior will be seen for SAEGW and S-GW + P-GW combination call.
	Accepted / Other GTP CCR-UCauses	**Important** If RAN/NAS cause is received in the delete bearer response that is initiated by the network through RAR/CCA-U, then P-GW will not send CCR-U to the PCRF to report the RAN/NAS cause. This support is introduced in 29.212 release 13.5 with "Enhance RAN/NAS" feature".

Table 12: Gz Interface Requirements for RAN/NAS Cause

Message	S-GW CDR	P-GW CDR
Delete Session Request	Yes	Yes
Delete Bearer Command	Yes	Yes NOTE: RAN/NAS cause if received in delete bearer response will overwrite the RAN/NAS cause received in delete bearer command
Failed Create Bearer Response	No	No
Failed Update Bearer Response	No	No
Delete Bearer Response	No	Yes

Limitations

Following are the limitations of this feature:

- Support of RAN/NAS cause over S2a and S2b interfaces is not supported.

- Support of RAN/NAS cause information has not been added for standard Gx and Gz dictionaries.
- P-GW processes first two RAN/NAS cause IE (max one RAN and max one NAS) information received from the GTP interface. For example, if the access network misbehaves and sends RAN/NAS cause list with two NAS and one RAN then only first two causes are considered and validated. In this case, these are two NAS causes, only first NAS cause will be populated at the Gx interface and in the CDRs as only one NAS is allowed.
- As per spec 32.251 Table 5.2.3.4.1.1 and Table 5.2.3.4.2.1, there is no trigger to generate the S-GW CDRs and P-GW CDRs for failed create bearer response and failed update bearer response. Hence, RAN/NAS cause received in "Failed Create Bearer" response and "Failed Update Bearer" response will not be sent to the Gz interface.
- In "Delete Bearer" scenario, S-GW CDRs are generated immediately after receiving "Delete Bearer" request. Hence, RAN/NAS cause received in the "Delete Bearer" response is not populated in the S-GW CDRs.
- If RAN/NAS cause is received in the "Delete Bearer" response that is initiated by the network through RAR/CCA-U, P-GW will not send CCR-U to the PCRF to report the RAN/NAS cause. This support is introduced in spec 29.212 release 13.5 with "Enhance RAN/NAS" feature".
- If the RAN-NAS-Cause feature is supported, only RAN/NAS cause is forwarded to PCRF . ANI information will be forwarded only when NetLoc feature is enabled. Below table describes various scenarios,

Scenario	RAN/NAS Cause Behavior	ANI Behavior
IP-CAN Bearer Termination	If the RAN-NAS-Cause feature is supported (If Netloc-ran-nas-cause CLI is configured and Supported-Features = RAN-NAS-CAUSE was asserted in the Gx CCR-I/CCA-I), PCEF will include the received RAN cause and/or the NAS cause due to bearer termination, in the RAN-NAS-Release-Cause AVP included in the Charging-Rule-Report AVP.	ANI information received during bearer termination is populated in the CCR-U, if Required-Access-Info was asserted when one or more of the failed charging rules installation request was received in CCA-U/RAR (If Netloc CLI is configured and Supported-Features = Netloc was asserted in Gx CCR-I/CCA-I).
IP-CAN Session Termination	If the RAN-NAS-Cause feature is supported (If Netloc-ran-nas-cause CLI is configured and Supported-Features = RAN-NAS-CAUSE was asserted in the Gx CCR-I/CCA-I), PCEF will include the received RAN cause and/or the NAS cause due to session termination, in the RAN-NAS-Release-Cause AVP at the command level.	ANI information received during session termination is populated in CCR-T, if Required-Access-Info was asserted when one or more of the failed charging rules installation request was received in the CCA-U/RAR (If Netloc CLI is configured and Supported-Features = Netloc was asserted in the Gx CCR-I/CCA-I).

Scenario	RAN/NAS Cause Behavior	ANI Behavior
PCC Rule Error Handling	If the RAN-NAS-Cause feature is supported (If Netloc-ran-nas-cause CLI is configured and Supported-Features = RAN-NAS-CAUSE was asserted in Gx CCR-I/CCA-I), PCEF will include the received RAN cause and/or the NAS cause due to rule installation/ activation/ modification failure, in the RAN-NAS-Release-Cause AVP included in the Charging-Rule-Report AVP.	ANI information received due to rule installation/activation/modification failure is populated in CCR-U, if Required-Access-Info was asserted when one or more of the failed charging rules installation request was received in CCA-U/RAR (If Netloc CLI is configured and Supported-Features = Netloc was asserted in the Gx CCR-I/CCA-I).

Command Changes

diameter encode-supported-features netloc netloc-ran-nas-cause

The behavior of this CLI command has been modified in this feature enhancement.

Previous Behavior: To enable the RAN/NAS Cause feature, it was mandatory to enable the NetLoc feature. For this, it was mandatory to configure the **netloc** keyword in the CLI command **diameter encode-supported-features netloc netloc-ran-nas-cause** .

New Behavior: Now, you can enable the RAN/NAS feature without configuring the NetLoc feature. This implied that it is not mandatory to configure the **netloc** keyword in the CLI command **diameter encode-supported-features netloc netloc-ran-nas-cause** .

```
configure > context context_name > ims-auth-service service_name > policy-control
 diameter encode-supported-features netloc netloc-ran-nas-cause
```

Session Disconnect During Diamproxy-Session ID Mismatch

This section describes how to clear the subscriber sessions that are impacted due to the mismatch in Diamproxy grouping information and Session ID.

This section discusses the following topics for this feature:

Feature Description

During rapid back-to-back ICSR switchovers or extensive multiple process failures, the Diameter proxy-Session manager mapping information is not preserved across ICSR pairs. This mismatch in the Diameter proxy-Session ID results in rejection of RAR with 5002 - DIAMETER_UNKNOWN_SESSION_ID cause code. This behavior impacts the VoLTE call setup procedure. Hence, this feature is introduced to clear the subscriber sessions that are impacted due to the mismatch in the Diameter proxy-session manager mapping. New CLI configuration

is provided to control the behavior and new bulk statistic counter is supported to report the Diamproxy-Session ID mismatch.

The bulk statistic counter will be incremented only when session is cleared upon receiving RAR message with 5002 result code and detecting session-ID Diamproxy mapping mismatch. A Delete Bearer Request is sent to S-GW with a Reactivation Requested as the cause code while suppressing the CCR-T from being sent to PCRF. So, the subscriber reattaches immediately without impacting the subsequent VoLTE calls, encountering only one failure instead of manual intervention.

Important This enhancement is applicable only to IMS PDN so that there is a limit of one failure when encountering this situation instead of manual intervention. This is applicable to only the Gx RARs.

Configuring System to Delete Diamproxy-Session ID Mismatched Sessions

The following section provides the configuration commands to enable the system to clear the subscriber sessions that are impacted due to the mismatch in Diamproxy grouping information and Session ID.

Clearing Mismatched Subscriber Sessions

Use the following configuration commands to configure the system to disconnect the subscriber sessions based on signaling trigger when session ID and Diamproxy mismatch is identified.

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
             diameter clear-session sessid-mismatch
end
```

- **sessid-mismatch**: Clears the session with mismatched session ID. This CLI configuration is optional.
- The default configuration is **no diameter clear-session**. By default, the sessions will not be cleared.

Verifying the Configuration to Delete Mismatched Sessions

Use the following command to verify the configuration status of this feature.

```
show ims-authorization service name service_name
```

service_name must be the name of the IMS Authorization service configured for IMS authentication.

This command displays all the configurations that are enabled within the specified IMS authorization service. The "Session-Id Mismatch Clear Session" field can be used to determine whether this feature is enabled or disabled.

```
[local]st40# show ims-authorization service name service1
  Context: test
  IMS Authorization Service name: service1
  Service State: Enabled
  Service Mode: Single Interface Policy and Charging
...
  Diameter Policy Control:
   Endpoint: gx
   Origin-Realm: xyz.com
   Dictionary: standard
```

```
    Supported Features:
       3gpp-r9
...
    Host Selection: Table: 1 Algorithm: Round-Robin
    Host Reselection Subscriber Limit: Not Enabled
    Host Reselection Interval: Not Enabled
    Sgsn Change Reporting: Not Enabled
      Session-Id Mismatch Clear Session: Enabled
    3GPP R9 Flow Direction Compliance: Not Enabled
  Host Selection Table[1]: 1 Row(s)
    Precedence: 1
...
```

Monitoring and Troubleshooting the Mismatched Session Deletion Feature

This section provides information regarding show commands and/or their outputs in support of this feature.

The following operations should be performed for any failure related to this feature:

- Verify if the feature is enabled using **show ims-authorization service name** <*service_name*> CLI command. If not enabled, configure the **diameter clear-session sessid-mismatch** CLI command and check if it works.
- Collect the output of **show ims-authorization policy-control statistics debug-info** and **show diameter statistics proxy debug-info** commands and analyze the debug statistics.
- Check the system logs that are reported while deleting the affected sessions. For further analysis, contact Cisco account representative.

show ims-authorization service name

A new field "Session-Id Mismatch Clear Session" is added to the output of this show command to indicate whether this feature is enabled or disabled within the specified IMS authorization service.

IMSA Schema

The following bulk statistic variable is added to this schema to report the Diamproxy-Session ID mismatch.

- dpca-rar-dp-mismatch - This counter displays the total number of sessions cleared while receiving RAR because of session-ID Diamproxy mapping mismatch.

Support for Negotiating Mission Critical QCIs

This section describes the overview and implementation of the Mission Critical QCIs Negotiation feature.

This section includes the following topics:

Feature Description

To support Mission Critical (MC) Push to Talk (PTT) services, a new set of standardized QoS Class Identifiers (QCIs) (65, 66, 69, 70) have been introduced. These are 65-66 (GBR) and 69-70 (non-GBR) network-initiated QCIs defined in 3GPP TS 23.203 v13.6.0 and 3GPP TS 23.401 v13.5.0 specifications. These QCIs are used for Premium Mobile Broadband (PMB)/Public Safety solutions.

Important The MC-PTT QCI feature requires Wireless Priority Service (WPS) license to be configured. For more information, contact Cisco account representative.

Previous Behavior: The gateway accepted only standard QCIs (1-9) and operator defined QCIs (128-254). If the PCRF sends QCIs with values between 10 and 127, then the gateway rejects the request. MC QCI support was not negotiated with PCRF.

New Behavior: PCRF accepts the new standardized QCI values 69 and 70 for default bearer creation and 65, 66, 69 and 70 for dedicated bearer creation.

For this functionality to work, a new configurable attribute, **mission-critical-qcis**, is introduced under the **diameter encode-supported-features** CLI command. When this CLI option is enabled, the gateway allows configuring MC QCIs as a supported feature and then negotiates the MC-PTT QCI feature with PCRF through Supported-Features AVP.

The gateway rejects the session create request with MC-PTT QCIs when the WPS license is not enabled and Diameter is not configured to negotiate MC-PTT QCI feature, which is part of Supported Feature bit.

For more information on this feature and associated configurations, refer to *P-GW Enhancements for 21.0* section in the *Release Change Reference* guide.

Configuring DPCA for Negotiating Mission Critical QCIs

The following section provides the configuration commands to enable support for MC-PTT QCI feature.

Enabling Mission Critical QCI Feature

Use the following configuration commands to enable MC-PTT QCI feature.

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
            diameter encode-supported-features mission-critical-qcis
            end
```

Notes:

- **mission-critical-qcis**: This keyword enables MC-PTT QCI feature. By default, this feature will not be enabled.
- This keyword can be enabled only if the WPS license is configured. For more information, contact your Cisco account representative.
- To disable the negotiation of this feature, the existing **no diameter encode-supported-features** command needs to be configured. On executing this command, none of the configured supported features will be negotiated with PCRF.

Verifying the Mission Critical QCI Feature Configuration

The **show ims-authorization sessions full all** command generates a display that indicates the configuration status of this feature.

The following sample display is only a portion of the output which shows *mission-critical-qcis* among the Negotiated Supported Features.

```
show ims-authorization sessions full all

 CallId: 00004e29            Service Name:  ims-ggsn-auth
   IMSI: 123456789012341
   ....

 Negotiated Supported Features:
   3gpp-r8
   mission-critical-qcis
 Bound PCRF Server: 192.1.1.1
 Primary PCRF Server: 192.1.1.1
 Secondary PCRF Server: NA
 ....
```

Monitoring and Troubleshooting the Mission Critical QCI

The following section describes commands available to monitor the Mission Critical QCI feature.

Mission Critical QCI Show Command(s) and/or Outputs

show ims-authorization sessions full all

On running the above mentioned show command, statistics similar to the following are displayed and will indicate if the Mission Critical QCI feature is enabled or not.

```
show ims-authorization sessions full all

 CallId: 00004e29            Service Name:  ims-ggsn-auth
   IMSI: 123456789012341
   ....

 Negotiated Supported Features:
   3gpp-r8
   mission-critical-qcis
   ....
```

HSS and PCRF-based P-CSCF Restoration Support for WLAN

This section describes the overview and implementation of the HSS-based and PCRF-based P-CSCF Restoration feature for WLAN and EPC networks.

This section includes the following topics:

Feature Description

The P-CSCF restoration procedures were standardized to minimize the time a UE is unreachable for terminating calls after a P-CSCF failure. In compliance with 3GPP standard Release 13, this feature is developed to include the following P-CSCF restoration mechanisms:

- HSS-based P-CSCF Restoration for Trusted/Untrusted WLAN Access (S2a/S2b)
- PCRF-based P-CSCF Restoration for LTE (S5/S8) and Trusted/Untrusted WLAN Access (S2a/S2b)

Important HSS-based P-CSCF Restoration was supported at P-GW for LTE (S5/S8) prior to StarOS release 21.0.

This feature provides support for both basic and extended P-CSCF Restoration procedures.

Important The P-CSCF Restoration is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

- **HSS-based P-CSCF Restoration for WLAN**:

  If the P-CSCF restoration mechanism is supported, gateway indicates the restoration support to AAA server through Feature-List AVP in the Authorization Authentication Request (AAR) message sent over S6b interface. The Feature-List AVP is part of the Supported-Features grouped AVP. The Bit 0 of the Feature-List AVP is used to indicate P-CSCF Restoration support for WLAN.

  During the P-CSCF Restoration, 3GPP AAA server, after having checked that the PGW supports the HSS-based P-CSCF restoration for WLAN, sends a P-CSCF restoration indication to the P-GW over S6b in a Re-authorization Request (RAR) command. A new Diameter AVP "**RAR-Flags**" is encoded in the RAR message with the Bit 1 set, would indicate to the gateway that the AAA server requests the execution of HSS-based P-CSCF restoration procedures for WLAN.

  The existing CLI command **diameter authentication** under AAA Group configuration is extended to encode P-CSCF Restoration feature as part of Supported-Features AVP in the AAR message.

  Important Supported-Features will be sent in every AAR message for RAT type WLAN. Feature negotiation is required in every AAR. ReAuth AAR will also do the feature renegotiation.

- **PCRF-based P-CSCF Restoration**:

  PCEF supporting P-CSCF restoration mechanism indicates the restoration support in CCR-I message through the Supported-Features AVP. The 24th Bit of the Supported-Feature-List AVP indicates whether this mechanism is supported or not.

  The existing CLI command **diameter encode-supported-features** in Policy Control configuration is extended to allow the negotiation of P-CSCF Restoration feature support with PCRF. A new Diameter AVP "**PCSCF-Restoration-Indication**" is introduced to indicate to PCEF that a P-CSCF Restoration is requested. This is achieved by setting AVP value to 0.

Supported-Features AVP is negotiated in CCR-I of all access types (eHRPD, P-GW, GGSN); however, Restoration trigger, if received, is ignored in eHRPD and GGSN.

Limitations

- As per the 3GPP standard specification, if S6b re-authorization request is used for P-CSCF Restoration for WLAN, then for extended P-CSCF Restoration the gateway may send authorization request with only mandatory AVPs. However, in the current implementation, ReAuth used for extended P-CSCF Restoration is a common authorization request of normal ReAuth. It will contain all the AVP of ReAuthorization AAR.

For more information on this feature and associated configurations, refer to *P-GW Enhancements for 21.0* and *SAEGW Enhancements for 21.0* section in the *Release Change Reference* guide.

Configuring the HSS/PCRF-based P-CSCF Restoration

The following section provides the configuration commands to enable support for HSS-based and PCRF-based P-CSCF Restoration feature.

Enabling P-CSCF Restoration Indication on S6b AAA interface

Use the following configuration commands for encoding Supported-Features AVP in the AAR message sent to AAA server via S6b interface.

```
configure
   context context_name
      aaa group group_name
         diameter authentication encode-supported-features
pcscf-restoration-indication
         end
```

Notes:

- **encode-supported-features**: Encodes Supported-Features AVP.
- **pcscf-restoration-indication**: Enables the P-CSCF Restoration Indication feature.
- **default encode-supported-features**: Configures the default setting, that is not to send the Supported-Features AVP in AAR message.
- **no encode-supported-features**: Disables the CLI command to not send the Supported-Features AVP.
- The **pcscf-restoration-indication** keyword is license dependent. For more information, contact your Cisco account representative.

Enabling P-CSCF Restoration Indication on Gx interface

Use the following configuration to enable P-CSCF Restoration Indication feature on Gx interface.

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
            diameter encode-supported-features pcscf-restoration-ind
            end
```

Notes:

- **pcscf-restoration-ind**: Enables the P-CSCF Restoration Indication feature. This keyword is license dependent. For more information, contact your Cisco account representative. By default, this feature is disabled.
- **default encode-supported-features**: The default configuration is to remove/reset the supported features.
- **no encode-supported-features**: Removes the previously configured supported features.

Verifying the HSS/PCRF-based P-CSCF Restoration

show ims-authorization sessions full all

This command generates a display that indicates the negotiation status of this feature.

The following sample display is only a portion of the output which shows **pcscf-restoration-ind** among the Negotiated Supported Features.

```
show ims-authorization sessions full all

CallId: 00004e22            Service Name:  imsa-Gx
  IMSI: 123456789012341
  ....
Negotiated Supported Features:
  3gpp-r8
  pcscf-restoration-ind
....
```

show aaa group all

This show command displays **pcscf-restoration-ind** as part of Supported-Features, if this feature is configured under AAA group.

```
show aaa group all
 Group name:    default
 Context:   local

 Diameter config:
  Authentication:
....
Supported-Features:   pcscf-restoration-ind
....
```

Monitoring and Troubleshooting the HSS/PCRF-based P-CSCF Restoration

This section provides information regarding show commands and/or their outputs in support of this feature.

The following operations can be performed for troubleshooting any failure related to this feature:

- Verify if the feature is enabled using **show ims-authorization sessions full all** and **show aaa group all** CLI commands. If not enabled, configure the required CLI commands both under Policy Control and AAA group configuration and check if it works.
- Execute **monitor protocol** command and check if the support for P-CSCF Restoration feature is negotiated in CCR-I and AAR messages. If not, enable the respective CLI commands for this feature to work.
- If the failure is still observed, obtain the following information and contact Cisco account representative for further analysis:

- Monitor protocol log with options 74 (EGTPC) and 75 (App Specific Diameter –Gx/S6b) turned on
- Logs with sessmgr, imsa, and diameter-auth enabled
- Output of **show session disconnect reason** CLI command and the relevant statistics at service level

Show Commands and/or Outputs

show ims-authorization sessions full all

The **Negotiated Supported Features** field in this show command output displays whether or not the P-CSCF Restoration feature is negotiated with PCRF.

This supported feature is displayed only when the feature license is configured.

show aaa group all

The **Supported Features** field in this show command output displays whether or not the P-CSCF Restoration feature is configured as part of the Supported-Features AVP.

This supported feature is displayed only when the feature license is configured.

show license information

If the license to enable the P-CSCF Restoration feature is configured, then the **show license information** command displays the associated license information.

Monitoring Logs

This section provides information on how to monitor the logs that are generated relating to the HSS/PCRF-based P-CSCF Restoration feature.

S6b Diameter Protocol Logs

The **Supported-Features** field is available in AAR/AAA section. The log output generated will appear similar to the following:

```
<<<<OUTBOUND  15:37:23:561 Eventid:92870(5)
....
 [V] [M] Supported-Features:
   [M] Vendor-Id: 10415
   [V] Feature-List-ID: 1
   [V] Feature-List: 1
....

INBOUND>>>>>  15:37:23:562 Eventid:92871(5)
....
 [V] [M] Supported-Features:
   [M] Vendor-Id: 10415
   [V] Feature-List-ID: 1
   [V] Feature-List: 1
....
```

The **RAR-Flags** field is available in RAR section. The log output generated will appear similar to the following:

```
INBOUND>>>>>  15:37:43:562 Eventid:92871(5)
....
[M] Re-Auth-Request-Type: AUTHORIZE_ONLY (0)
[V] RAR-Flags: 2
....
```

Gx Diameter Protocol Logs

Under **Supported-Features**, the P-CSCF Restoration **Feature-List** is available in CCR-I/CCA-I section. The output generated will appear similar to the following:

```
<<<<OUTBOUND  13:52:06:117 Eventid:92820(5)
....
 [V] [M] Supported-Features:
   [M] Vendor-Id: 10415
   [V] Feature-List-ID: 1
    [V] Feature-List: 16777217
....
INBOUND>>>>>  13:52:06:118 Eventid:92821(5)
....
 [V] [M] Supported-Features:
   [M] Vendor-Id: 10415
   [V] Feature-List-ID: 1
    [V] Feature-List: 16777216
....
```

The **PCSCF-Restoration-Indication** AVP is available in RAR. The output generated will appear similar to the following:

```
INBOUND>>>>>  13:52:26:119 Eventid:92821(5)
....
[M] Re-Auth-Request-Type: AUTHORIZE_ONLY (0)
[V] PCSCF-Restoration-Indication: 0
....
```

Loop Prevention for Dynamic Rules

Feature Information

Summary Data

Status	New Functionality
Introduced-In Release	21.2
Modified-In Release(s)	Not Applicable
Applicable Product(s)	P-GW
Applicable Platform(s)	ASR 5500
Default Setting	Disabled
Related CDETS ID(s)	CSCvc97345, CSCvd02249
Related Changes in This Release	Not Applicable
Related Documentation	P-GW Administration Guide Command Line Interface Reference

Revision History

Important Revision history details are not provided for features introduced before release 21.2.

Revision Details	Release	Release Date
New in this release.	21.2	April 27, 2017

Feature Description

When a PCC (Dynamic or Predefined) rule installation fails, the PCEF initiates a CCR-U toward the PCRF to report the failed rule. In case the PCRF responds back with same rule definition, then the rule failure CCR-U is initiated again. This results in a loop of rule failure.

With this feature, gateways have the ability to prevent the loop by reporting the rule install failure to PCRF only once until it is successfully installed.

How It Works

This feature is configurable through a CLI command with which, once a failure is being reported for a subscriber, failure for the same rule is suppressed for that subscriber until it is installed successfully. The rulenames are preserved for a subscriber for which the failures are reported. However, when the condition of the rule failure is rectified for an error (for example, rule definition is added to the configuration and the rule is successfully installed), then the gateway removes the rulename from the failed rules list. So, if the failure for that particular rule occurs again, it is reported to the PCRF.

The failed rulename is not checkpointed and so, if a recovery event like session recovery or an ICSR occurs then the failure of these rules are reported once again.

Configuring Loop Prevention for Dynamic Rules

This section explains the configuration procedures required to enable the feature.

Enabling ACS Policy to Control Loop Prevention

Use the following commands under ACS Configuration Mode to enable or disable the feature which prevents the rule failure loop between PCRF and PCEF:

```
configure
  active-charging service<service_name>
      policy-control report-rule-failure-once
      end
```

Notes:

- When configured, CCR-U will be sent only once for the same rule failure.
- By default, the feature is disabled.
- If previously configured, use the **no policy-control report-rule-failure-once** to disable the feature.

Monitoring and Troubleshooting

The following sections describe commands available to monitor the feature.

Show Commands and Outputs

This section provides information regarding show commands and their outputs for the Loop Prevention for Dynamic Rules feature.

show active-charging service all

The output of the above command has been enhanced to display the status (Enabled/Disabled) of the feature. For example:

```
show active-charging service all
  .
  .
  .
  Report Rule Failure Once: Enabled
```

show active-charging subscribers full all

The output of the above command has been enhanced to display the new parameter which shows the total number of rule failures not reported. For example:

```
 Callid:                         4e21        ACSMgr Card/Cpu:            15/0
 Active Charging Service name:                                           acs
 Active charging service scheme:
 ACSMgr Instance:                 1          Number of Sub sessions:     1
 Data Sessions Active:            0          Dynamic Routes created:     0
 Uplink Bytes:                    0          Downlink Bytes:             0
 Uplink Packets:                  0          Downlink Packets:           0
 Accel Packets:                   0
 FastPath Packets:                0
 Total NRSPCA Requests:           0          NRSPCA Req. Succeeded:      0
 NRSPCA Req. Failed:              0
 Total NRUPC Requests:            0          NRUPC Req. Succeeded:       0
 NRUPC Req. Failed:               0
 Pending NRSPCA Requests:         0          Pending NRUPC Requests:     0
 Total Bound Dynamic Rules:       0          Total Bound Predef. Rules:  0
 Data Sessions moved:             0
 Bearers Terminated for no rules:                                        0
 Failed Rulebase Install (unknown bearer-id):                            0
 Failed Rule Install (unknown bearer-id):                                0
 Total number of rule failures not reported:                             1
```

show active-charging subsystem all

The output of the above command has been enhanced to display the new parameter which shows the total number of rule failures not reported. For example:

```
 Total ACS Managers:           2
 Session Creation Succ:        1      Session Creation Fail:      0
 .
 .
 .
 Total Number of Unsolicited Downlink packets received : 0
 Total Number of ICMP-HU packets sent :                  0
```

```
RADIUS Prepaid Statistics:
Total prepaid sess:            0      Current prepaid sess:       0
Total prepaid auth req:        0      Total prepaid auth success: 0
Total prepaid auth fail:       0      Total prepaid errors:       0
Total number of rule failures not reported :           4

Content Filtering URL Cache Statistics:
Total cached entries:          0
Total hits:                    0      Total misses:               0
.
.
.
```

Separation of Accounting Interim Interval Timer for RADIUS and Diameter Rf

Feature Information

Summary Data

Status	New Functionality
Introduced-In Release	21.2
Modified-In Release(s)	Not Applicable
Applicable Product(s)	eHRPD, GGSN, P-GW
Applicable Platform(s)	ASR 5500
Default Setting	Disabled
Related CDETS ID(s)	CSCvc97616
Related Changes in This Release	Not Applicable
Related Documentation	AAA Interface Administration and Reference Command Line Interface Reference

Revision History

Important Revision history details are not provided for features introduced before release 21.2.

Revision Details	Release	Release Date
New in this release.	21.2	April 27, 2017

Feature Description

Prior to Release 21.2, the Cisco StarOS platform had a single configuration parameter for sending accounting interim records to RADIUS and Diameter Rf servers. Consequently, it was not possible to send accounting

interim records to RADIUS and Diameter Rf servers with different intervals using the available CLI options. This feature provides a CLI controlled mechanism to have different interim intervals for Diameter Rf and RADIUS accounting applications. Having a separate configurable CLI and interim interval timer values for RADIUS and Diameter Rf servers provides enhanced usability.

How It Works

Currently, the Diameter accounting uses the value configured for RADIUS accounting interim interval. With this feature, configurable through a CLI command, provides an option to separately configure Diameter accounting interim interval for Rf interface. Until Diameter interim CLI is configured with either "**no**" option or any specific timer value, as a measure for compatibility, RADIUS interim interval value is used for Diameter interim interval. Once Diameter configuration takes effect, any change to RADIUS configuration will not affect Diameter configuration and vice versa. The following table shows the Diameter interim interval values used for different scenarios.

Radius Configuration	Diameter Configuration	Diameter Interim Behavior
No configuration OR Interim Interval: X OR Interim disabled	Interim Interval: Y	Interim Interval: Y Note: X may or may not be same as Y
No configuration OR Interim Interval: X OR Interim disabled	Interim disabled using "No" option	Interim disabled
No configuration OR Interim Interval: X OR Interim disabled	No configuration	Fallback to RADIUS configuration

- Recovery/ICSR behavior: Interim interval configuration used at the time of PDN creation is applicable for entire lifetime of PDN. Recovery/ICSR will not have any impact of existing PDN behavior with regard to Diameter interim interval.
- ICSR Upgrade/Downgrade behavior:
  - Existing session will be recovered based on RADIUS configuration present in old chassis.
  - New session behavior is as per configuration available on newly active chassis.

Limitations

Following are the known limitations of this feature:

1. In case Diameter interim interval CLI is not configured, the P-GW retains the older behavior where Diameter accounting uses the same interim interval value configured for RADIUS accounting.
2. Once diameter accounting configuration is done, it's not possible to go back to the older behavior.

Configuring Diameter Accounting Interim Interval

Use the following commands under AAA Server Group Configuration Mode to configure Diameter accounting interim interval independently from RADIUS accounting interim interval:

```
configure
    context context_name
       aaa group group_name
          diameter accounting interim interval interval_in_seconds
          end
```

Notes:

- *interval_in_seconds:* Specifies the interim interval, and must be in the range of 50 through 40000000.
- If previously configured, use the **no diameter accounting interim interval** to disable the interim accounting messages on Rf interface.
- There is no default Diameter interim interval value.
- In case Diameter interim interval CLI is not configured, the P-GW retains the older behavior where Diameter accounting uses RADIUS interim interval configuration available in AAA server group configuration block.

Monitoring and Troubleshooting

The following sections describe commands available to monitor the feature.

Show Commands and Outputs

This section provides information regarding show commands and their outputs in support of the feature.

show aaa group { name <group_name> | all }

The output of the above command is modified to display the following new field to show the current configuration for interim interval used for upcoming Diameter Rf accounting sessions:

- Interim-timeout: <50-40000000> or <None>

Following is a sample output where Diameter interim interval is not configured:

```
show aaa group name default
Group name:                   default
Context:                      pgw

Diameter config:
  Accounting:
```

```
      Request-timeout:          20
      Interim-timeout:          None
```

Following is a sample output where Diameter interim interval is configured with the value 900:

```
show aaa group name default
Group name:                     default
Context:                        pgw

Diameter config:
  Accounting:
    Request-timeout:            20
    Interim-timeout:            900
```

show configuration [verbose]

The output of the above command is modified to display the following new field to show the interval of interim messages in seconds:

- diameter accounting interim interval <*value_in_seconds*>

Following is a sample output where Diameter interim interval is configured with the value 60:

```
show configuration context isp verbose
config
    context isp
        aaa group default
            diameter accounting interim interval 60
```

Enhancement to OCS Failure Reporting for Gy

Feature Information

Summary Data

Status	Modified Functionality
Introduced-In Release	21.1
Modified-In Release(s)	21.2
Applicable Product(s)	P-GW, SAEGW
Applicable Platform(s)	ASR 5500
Default Setting	Enabled
Related CDETS ID(s)	CSCvc93904
Related Changes in This Release	Not Applicable
Related Documentation	AAA Interface Administration and Reference P-GW Administration Guide SAEGW Administration Guide

Revision History

Important Revision history details are not provided for features introduced before release 21.2.

Revision Details	Release	Release Date
New in this release.	21.2	April 27, 2017

Feature Description

When Cisco-Event-Trigger-Type AVP is installed by PCRF in CCA-I, CCA-U or in RAR messages with value CREDIT_CONTROL_FAILURE (5), then the Cisco-Event grouped AVP is sent by the P-GW to PCRF in CCR-U message with the exact value of OCS failure code. This trigger is sent only when Gy failure occurs and based on the configuration (Credit-Control-Failure-Handling), the 'Continue' action is taken and Gy session moves to Offline state.

In releases prior to the implementation of this enhancement, if a failure code was received from OCS in the range of 3000-3999, then Cisco-CC-Failure-Type was sent with the value 3XXX. Similarly, for error codes in the range of 4000-4999 or 5000-5999, Cisco-CC-Failure-Type was reported as 4XXX or 5XXX respectively. With this enhancement, the exact failure code is reported to the PCRF instead of the range. For example, when the Cisco-Event-Trigger-Type is CREDIT_CONTROL_FAILURE (5) and OCS failure code is 3002 in CCA-U, then in CCR-U towards PCRF Cisco-CC-Failure-Type (as part of grouped AVP Cisco-Event) is sent with a value of 3002.

Support Added for RAN/NAS Cause Code for S5/S8 and S2b Interfaces

Feature Information

Summary Data

Status	Modified Functionality
Introduced-In Release	21.1
Modified-In Release(s)	21.2
Applicable Product(s)	P-GW, S-GW, SAEGW
Applicable Platform(s)	ASR 5500
Default Setting	Disabled
Related CDETS ID(s)	CSCuy93748/CSCvc97356
Related Changes in This Release	Not Applicable

Related Documentation	*P-GW Administration Guide* *S-GW Administration Guide* *SAEGW Administration Guide* *Command Line Interface Reference*

Revision History

Important Revision history details are not provided for features introduced before Release 21.2.

Revision Details	Release	Release Date
New in this release.	21.2	April 27, 2017

Feature Changes

Important This is a license controlled feature. There are separate licenses for this feature. You must enable the existing license of NPLI or contact your Cisco account representative for information on how to obtain the custom license.

For billing co-ordination at IMS domain and VoWiFi deployments, an operator may require access to the RAN or NAS (or both) release cause code information available at P-CSCF. The P-GW provides detailed RAN/NAS cause information with ANI information received from the access network to the P-GW and further down to the PCRF based on the following events:

- Bearer deactivation (Delete Bearer Response/Delete Bearer Command)
- Session deactivation (Delete Session Request)
- Bearer creation/modification failures (Create/Update Bearer Response with cause as FAILURE)

The IMS network can retrieve detailed RAN and/or NAS release cause codes information from the access network that is used for call performance analysis, user QoE analysis, and proper billing reconciliation. This feature is supported on the S5, S8, Gx, and S2b interfaces.

This feature includes support RAN/NAS cause IE in Create Bearer Response, Update Bearer Response, Delete Bearer Response, Delete Bearer Command, and Delete Session Request. The following table shows the supported protocol type for RAN/NAS cause IE.

Table 13: Protocol Type for RAN/NAS IE

Interface	Supported Protocol Type for RAN/NAS IE
S5/S8	S1AP Cause (1)/EMM Cause (2)/ESM Cause (3)
S2b	Diameter Cause (4)/IKEv2 Cause (5)

Note Any protocol type value that is received apart from the supported protocol type values listed in the table are ignored and not forwarded to the PCRF.

GTP interface Requirements for RAN/NAS Cause

For S5/S8 interface, RAN/NAS cause is supported for the following messages for the dpca-custom8 dictionary.

- Failed Create Bearer Response
- Failed Update Bearer Response
- Delete Session Request
- Delete Bearer Response
- Delete Bearer Command

For S2b interface, RAN/NAS cause is supported for the following messages for the custom dpca-custom8 dictionary:

- Failed Create Bearer Response
- Failed Update Bearer Response
- Delete Session Request

Gx interface Requirements for RAN/NAS Cause

The RAN/NAS cause is added for the custom dpca-custom8 dictionary to ensure that the RAN/NAS cause is populated. The Gx interface behavior to handle RAN/NAS cause is as follows:

Table 14: Gx Interface Requirements for RAN/NAS Cause

Message	GTP Cause	Gx Message Carrying RAN-NAS Cause Information
Create Bearer Response	Accepted	RAN/NAS cause is not expected as per 29.274 Table 7.2.4-2. Therefore, if it is received, it is ignored and not forwarded to the PCRF.
	Temporarily rejected due to HO in progress.	RAN/NAS cause with this GTP cause is not applicable as per 29.274 Table C.4. Therefore, if it is received, it is ignored and not forwarded to the PCRF.
	Other GTP Causes	CCR-U

Message	GTP Cause	Gx Message Carrying RAN-NAS Cause Information
Update Bearer Response	Accepted	RAN/NAS cause is not expected as per 29.274 Table 7.2.16-2. Therefore, if it is received, it is ignored and not forwarded to the PCRF.
	No Resources Available	CCR-U **Note** If UE-initiated (MBC) bearer modification fails with GTP cause “NO RESOURCES AVAILABLE”, P-GW deletes the entire PDN session. In this case, RAN-NAS cause information is forwarded as part of CCR-T message.
	Context Not Found	CCR-U **Note** If the Update Bearer Response is received with the message level cause as "CONTEXT NOT FOUND", which leads to the PDN deletion, then the RAN-NAS cause information is forwarded as part of the CCR-T message.
	Temporarily rejected due to HO in progress.	RAN/NAS cause with this GTP cause is not applicable as per 29.274 Table C.4. Therefore, if it is received, it is ignored and not forwarded to the PCRF.
	Other GTP Causes	CCR-U

Message	GTP Cause	Gx Message Carrying RAN-NAS Cause Information
Delete Bearer Response	Temporarily rejected due to HO in progress	RAN/NAS cause with this GTP cause is not applicable as per 29.274 Table C.4. Therefore, if it is received, it is ignored and not forwarded to the PCRF. **Note** • If RAN/NAS cause is received in the Delete Bearer Response, which is triggered as a part of the Delete Bearer command and cause as “Request Accepted”, P-GW forwards the RAN/NAS cause (received in Delete Bearer Response) to the PCRF. • If RAN/NAS cause is received in the Delete Bearer command and Delete Bearer Response with HO in progress, the RAN/NAS Cause received in the Delete Bearer command is forwarded to the PCRF. • If RAN/NAS Cause is received in the Delete Bearer command and Delete Bearer Response with Accepted/Other Cause and new RAN/NAS Cause, the new RAN/NAS cause is forwarded to the PCRF.
	Accepted / Other GTP CCR-UCauses	CCR-U **Note** If RAN/NAS cause is received in the delete bearer response that is initiated through RAR/CCA-U, then P-GW doesl not send CCR-U to the PCRF to report the RAN/NAS cause. This support is introduced in 29.212 release 13.5 with "Enhance RAN/NAS" feature".
Delete Session Request	Accepted	CCR-T

ANI Behavior Towards PCRF

Section 4.5.6, 4.5.7, 4.5.12 of 3GPP 29.212 v13.4.0 mentions that if the RAN-NAS-Cause feature is supported, the PCEF should provide the available access network information within the 3GPP-User-Location-Info AVP (if available), TWAN-Identifier (if available and Trusted-WLAN feature is supported), User-Location-Info-Time AVP (if available), and 3GPP-MS-TimeZone AVP (if available).

In the earlier releases, the dpca-custom8 dictionary did not support USER-LOCATION-INFO-TIME AVP.

In this release, the USER-LOCATION-INFO-TIME AVP is added to the dpca-custom8 dictionary, which is sent to the PCRF (if available) as a part of ANI. Also, new PROTOCOL-TYPE, 1 to 5 are supported for RAN/NAS. This AVP can be seen in the CCR-U and CCR-T (whenever applicable). Also the new PROTOCOL-TYPE (S1AP Cause, EMM Cause, ESM Cause, IKEv2, DIAMETER) is visible on the Gx interface (if the same is received over the S5/S8/S2b interface).

ANI Behavior for S5/S8 Interface

Along with RAN/NAS cause, P-GW also sends following information to the PCRF, if available, for the dpca-custom8 dictionary:

Table 15: Mapping of GTP IE to ANI AVPs on Gx Interface

GTP IE	Gx AVP
UE Time Zone	3GPP-MS-TimeZone
ULI Timestamp	User-Location-Info-Time
User Location Information	3GPP-User-Location-Info

ANI information is sent to the PCRF irrespective of the event triggers configured when the RAN/NAS feature is enabled.

ANI Behavior for S2b Interface

ANI information is not sent towards PCRF for the dpca-custom8 dictionary. Also, the TWAN-Identifier is not supported as part of ANI for the dpca-custom8 dictionary.

Limitations

Following are the limitations of this feature:

- Support of RAN/NAS cause information is added only for the dpca-custom8 dictionary.
- PGW processes first two RAN/NAS cause IE (max one RAN and max one NAS) information received from the GTP interface. For example, if the access network misbehaves and sends RAN/NAS cause list with two NAS and one RAN then only first two causes are considered and validated. In this case, there are two NAS causes, only first NAS cause is populated at the Gx interface.
- RAN/NAS information is populated only on the Gx interface, no other interface is impacted.

Command Changes

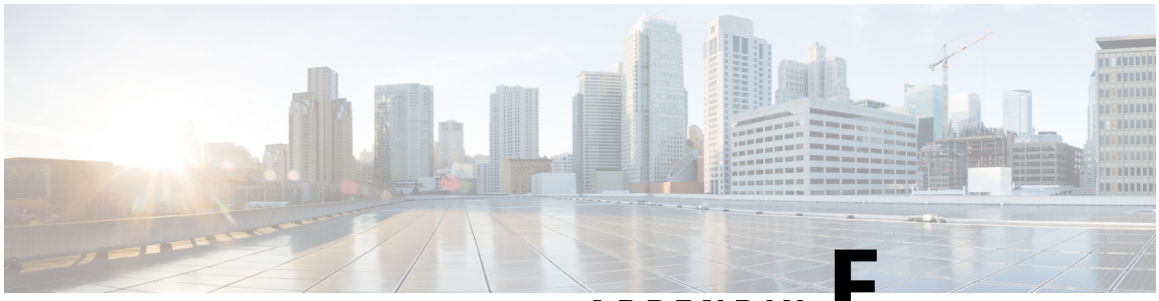
diameter encode-supported-features netloc-ran-nas-cause

Use the existing CLI command, **diameter encode-supported-features netloc-ran-nas-cause** to enable the RAN/NAS cause on each of the S5/S8 and S2b interfaces.

This feature is disabled by default.

To enable this feature, enter the following commands:

```
configure
  context ISP1
     ims-auth-service IMSGx
       policy-control
       diameter encode-supported-features netloc-ran-nas-cause
       end
```



APPENDIX E

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 system 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 the administration guide for the product that you are deploying.

Introduction

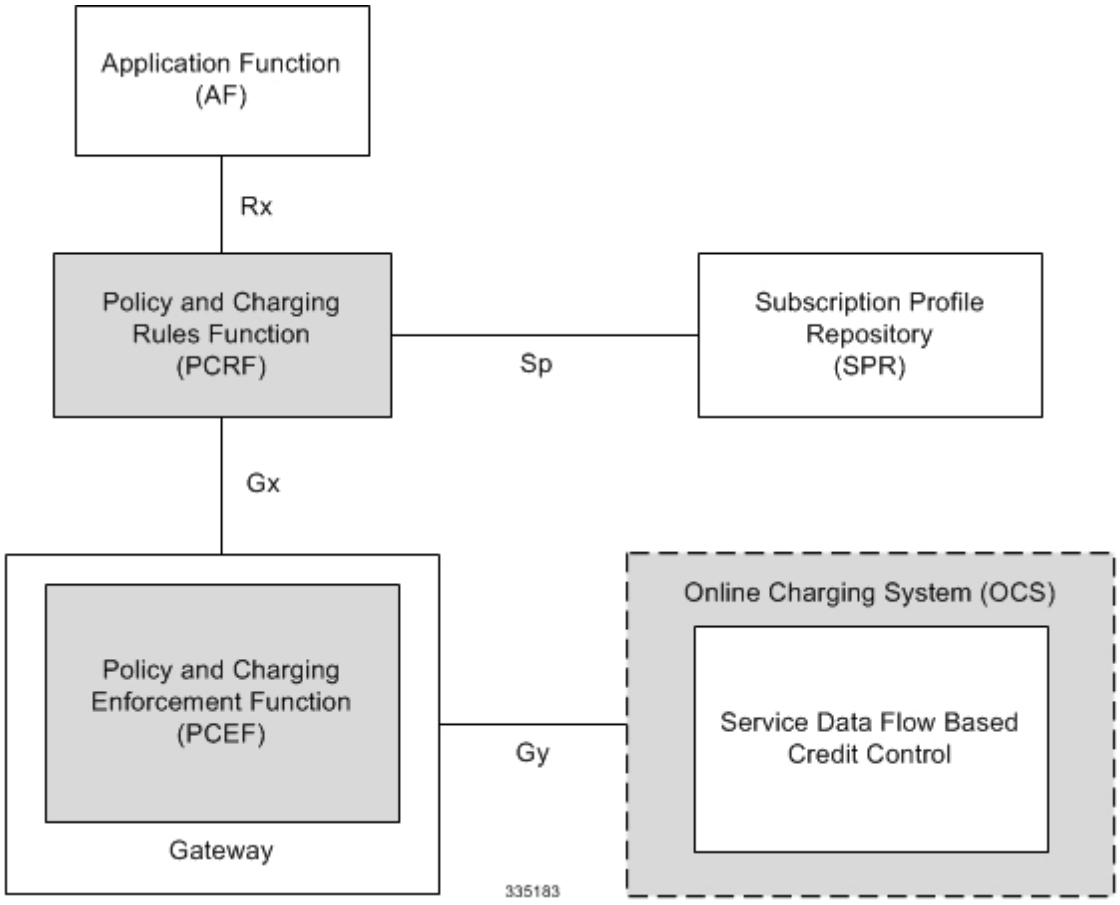
The Gy interface is the online charging interface between the PCEF/GW (Charging Trigger Function (CTF)) and the Online Charging System (Charging-Data-Function (CDF)).

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.

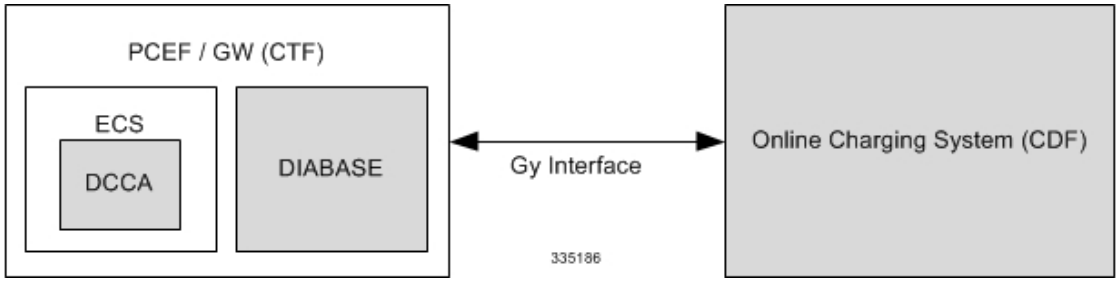
The following figure shows the Gy reference point in the policy and charging architecture.

Figure 15: 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 16: Gy Architecture



License Requirements

The Gy interface support is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on

installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *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 does not 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.

  In releases prior to 17.0, the AVP "SN-Remaining-Service-Unit" was not sent in the CCR-T and CCR-U messages with reporting Reason FINAL when the FUI action was received as Redirect and the granted units was zero in CCA. In 17.0 and later releases, for the Final-Reporting, the AVP "SN-Remaining-Service-Unit" will be encoded.

The "SN-Remaining-Service-Unit" AVP behavior is inherited from "Used-Service-Unit" AVP. This Final-Reporting is missing for the Remaining-Service-Unit AVP, which is now incorporated.

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 (RSU) 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.

In 12.3 and earlier releases, when no pre-emptive quota request is present in CCR-I, on hitting server unreachable state for initial request, MSCC AVP with RSU is present in the CCR-I on server retries. Release

14.0 onwards, the MSCC AVP is skipped in the CCR-I on server retries. Corresponding quota usage will be reported in the next CCR-U (MSCC AVP with USU and RSU).

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, traffic 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 is 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-U 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)

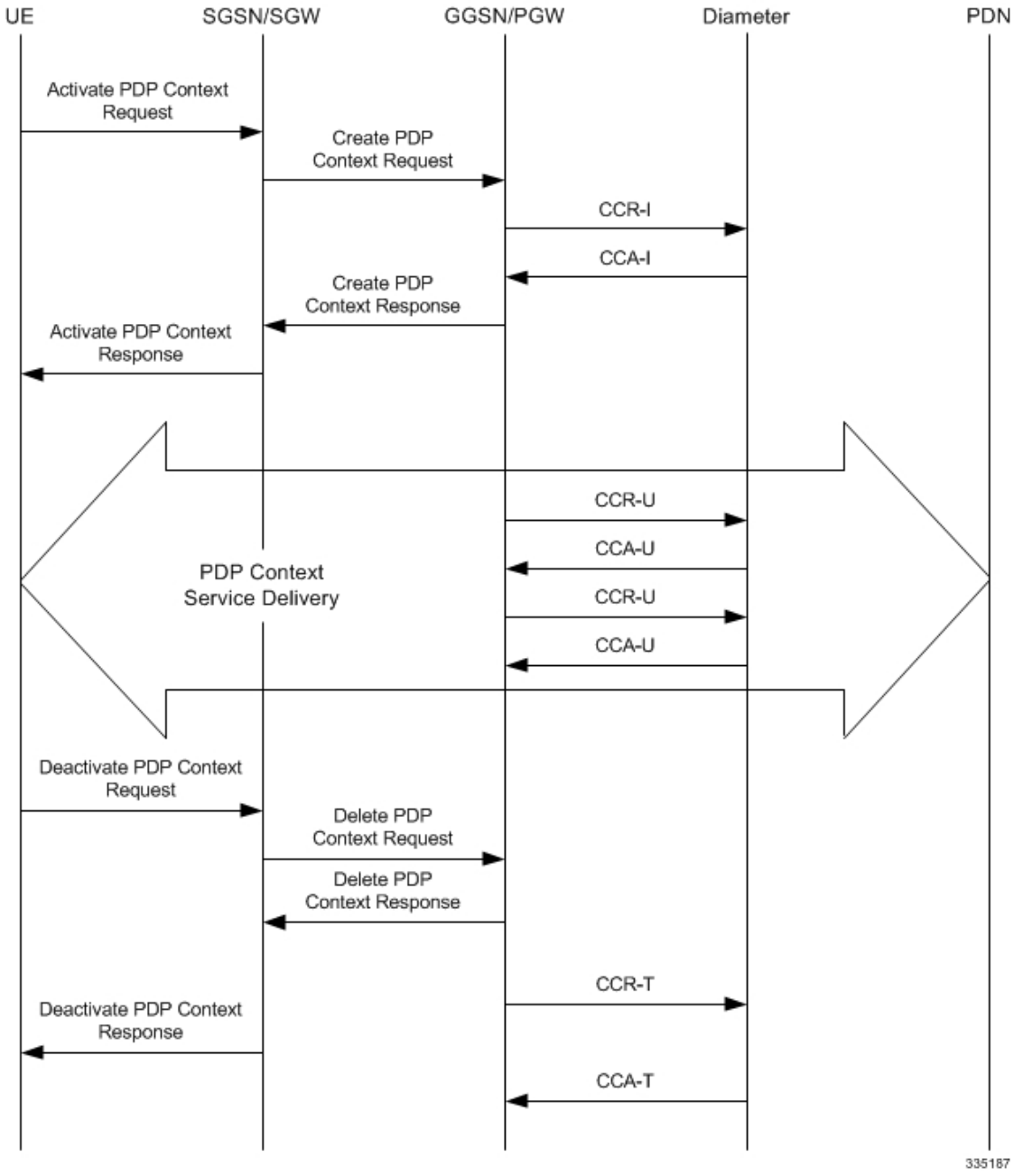
  If the MSCC AVP is missing in CCA-U it is treated as invalid CCA and the session is terminated.
- Credit Control Answer - Terminate (CCA-T)

In releases prior to 16.0, CCR-T was immediately sent without waiting for CCA-U if the call was cleared and there was a pending CCA-U. In 16.0 and later releases, if call is cleared when there is a pending update, the gateway will wait for CCA-U to arrive or timeout to happen (whichever happens first).

In releases prior to 20, CCR-Ts were not reported over Gy interface when the calls were terminated due to audit failure during ICSR switchover. In 20 and later releases, DCCA allows generation of CCR-Ts in this scenario.

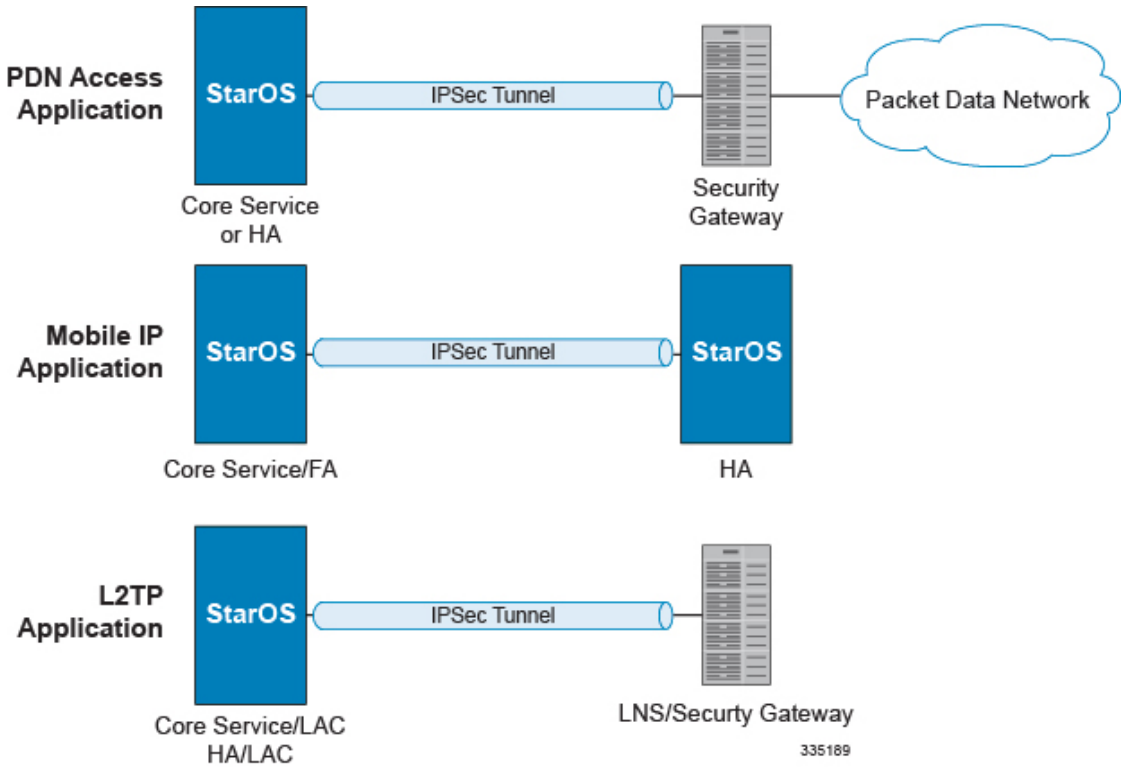
The following figure depicts the call flow for a simple call request in the GGSN/P-GW/IPSG Gy implementation.

Figure 17: Gy Call Flow for Simple Call Request for GGSN/P-GW/IPSG



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

Figure 18: Gy Call Flow for Simple Call Request for HA



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.

In releases prior to 16.0, once a CCR-U was sent out over Gy interface, ACR-I message was immediately triggered (or containers were cached) based on policy accounting configuration and did not wait for CCA-U. In 16.0 and later releases, containers are closed only after CCA-U is received successfully. That is, Rf trigger will be sent only after receiving CCA-U message.

Redirection

In the Final-Unit-Indication AVP, if the Final-Unit-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-Unit-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, on page 212.

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.

Important The DCCA supports maximum of three bearers (including default) for the ICSR Checkpointing and Recovery. When more than three bearers are configured in the DCCA, checkpointing occurs from Active to Standby for all the bearers. However, during recovery, only the first three bearers are recovered and the rest remain in the memory consuming resources.

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

Error Mechanisms

Following are supported 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

Gy Interface Support

- 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

PLMN and Time Zone Reporting

For some implementations of online charging, the OCS requires the PCEF to reporting location-specific subscriber information. For certain subscriber types, subscriber information such as PLMN, Time Zone, and ULI can be sent over the Gy interface as the subscriber changes location, time zone, and serving networks to provide accurate online charging services. Such information can be reported independently from time and volume-based reporting.

PLMN and Time Zone Reporting feature is enabled to support location event reporting based on triggers from Gx, when the following conditions are met:

- Session-based Gy is not initiated due to the absence of charging-actions in rulebase with Credit-Control enabled or due to delayed Gy session initiation.
- PLMN and Time Zone Reporting feature is either enabled in the credit control group or through the use of triggers received from Gx.

If session-based Gy initiation fails or the session goes offline due to configuration or network issues, event-based Gy session will not be initiated.

Important Note that the failure-handling will not be supported for event-based Gy.

Though, in event-based Gy, multiple events can be reported independently and simultaneously this is presently not supported. If an event occurs when the CCA-Event (CCA-E) of the previously reported event is awaited, then the new event is queued and reported only when a CCA-E is received or the message is timed out.

To enable the PLMN and Time Zone Reporting feature, the PCRF shall send the Trigger AVP (Trigger Type 1, Trigger Type 2) at the command level in a CCA.

The Event-based Gy session will be terminated in the following scenarios:

- On termination of the bearer/subscriber (subscriber level Gy).
- Initiation of session-based Gy session (delayed session initiation).
- Once the CCR-E transaction is complete and there are no further events to report.

For information on how to configure this feature, refer to the *Gy Interface Support* chapter in the administration guide for the product that uses the Gy interface functionality.

Interworking between Session-based Gy and Event-based Gy

If both session-based Gy and event-based Gy mode are activated, then session-based Gy will take precedence i.e. all the events will be reported through CCR-U if the corresponding triggers are enabled. Event-based Gy mode will be active only when session-based Gy has been disabled and has never been activated previously for this session during its lifetime.

OCS Unreachable Failure Handling Feature

The OCS Unreachable Failure Handling feature is required to handle when OCS goes down or unavailable. This feature is otherwise noted as Assume Positive for Gy.

The OCS is considered unavailable/unreachable in the following scenarios:

- PCEF transmits a CCR-U or CCR-I message but no response is received before the specified timeout
- Diameter Watchdog request times out to the current RDR, causing the TCP connection state to be marked down
- Diameter command-level error codes received in a CCA
- If the PCEF is unable to successfully verify transmission of a CCR-T, the PCEF will not assign interim quota, because the user has disconnected.

In 15.0 and later releases, the error result codes can be configured using the CLI command **servers-unreachable behavior-triggers initial-request { result-code { any-error | result-code [to end-result-code] } }** to trigger the server unreachable mode. The same is applicable for the update request also. For more information on the CLI command, see the *Credit Control Configuration Mode Commands* chapter of the *Command Line Interface Reference*. However, if the CLI command **no servers-unreachable behavior-triggers { initial-request | update-request } result-code { any-error | result-code [to end-result-code] }** is configured, then the default set of hard-coded error codes are applicable.

The default set is:

- UNABLE_TO_DELIVER 3002
- UNABLE_TOO_BUSY 3004
- LOOP_DETECTED 3005
- ELECTION_LOST 4003
- Permanent failures 5001-5999 except 5002, 5003 and 5031.

In 12.2 and later releases, existing failure handling mechanism is enhanced such that the subscriber can be allowed to browse for a pre-configured amount of interim-volume and/or interim-time if OCS becomes unreachable due to transport connection failure or gives an impression that OCS is unreachable owing to slow response for Diameter request messages.

The purpose of this feature is to support Gy based data sessions in the event of an OCS outage. Diameter client allows the user's data session to continue for some fixed quota and then retries the OCS server to restore normal functionality. This feature adds more granularity to the existing failure handling mechanism.

With the implementation of this feature, Gy reporting during outages is supported. A temporary time and/or volume quota is assigned to the user in the event of an OCS outage which will be used during the outage period.

When the OCS returns to service, the GW reports all used quota back to OCS and continues with normal Gy reporting.

For each DCCA-service, CLI control is available for the following options:

- Interim quota volume (in bytes) and quota time (seconds). Both values will apply simultaneously, if configured together and if either quota time or quota volume is exhausted, the Diameter client retries the OCS.
- Option to limit the number of times a session can be assigned a temporary quota. If the user exceeds this amount, the session will be terminated/converted to postpaid.

The quota value is part of the dcca-service configuration, and will apply to all subscribers using that dcca-service. The temporary quota will be specified in volume (bytes) and/or time (seconds) to allow enforcement of both quota tracking mechanisms individually or simultaneously.

When a user consumes the interim total quota or time configured for use during failure handling scenarios, the GW retries the OCS server to determine if functionality has been restored. In the event that services have been restored, quota assignment and tracking will proceed as per standard usage reporting procedures. Data used during the outage will be reported to the OCS.

In the event that the OCS services have not been restored, the GW re-allocates the configured amount of quota and/or time to the user. The GW reports all accumulated used data back to OCS when OCS is back online. If multiple retries and interim allocations occur, the GW reports quota used during all allocation intervals. This cycle will continue until OCS services have been successfully restored, or the maximum number of quota assignments has been exhausted.

Support for OCS unreachable CLI commands is added under Diameter Credit Control Configuration mode.

For the P-GW/XGW/GGSN, this behavior will apply to all APNs and subscribers that have online charging enabled by the PCRF. In the HA, this behavior will apply to all users that have online charging enabled by the AAA. Settings will be applied to the dcca-service.

In Release 15.0, the following enhancements are implemented as part of the Assume Positive Gy feature:

- Configurable per error code treatment to enter assume positive mode
- Graceful session restart upon receipt of a 5002 error

Important Note that the Graceful session restart feature is customer specific. For more information contact your Cisco account representative.

Configurable per Error Code Treatment

This feature allows the customers to configure error result codes using the CLI command "**servers-unreachable behavior-triggers**" that will trigger entering assume positive mode on the fly for CCR-Initial and CCR-Update messages. CCR-Terminate message is currently not supported.

Any error result codes from the range 3xxx to 5xxx can be specified using the CLI commands. This feature has been implemented to provide more flexibility and granularity in the way assume positive mode is triggered for error result codes.

Graceful Session Restart

Graceful session restart upon receipt of a 5002 error code is supported for server retried CCR-U messages during assume positive state. Also, any unreported usage from the time, server retried CCR-U sent till CCA-I is received, will be reported immediately by triggering CCR-U with usages for the same.

Important Note that the Graceful session restart feature is customer specific. For more information contact your Cisco account representative.

Any pending updates are aborted once CCA-U with 5002 is received from the server. Also CCR-U is triggered immediately following session restart only if there are any unreported usages pending.

Important When the server responds with 5002 error result code, it does not include any granted service units for the requested rating groups.

For more information on the commands introduced in support of this feature, see the *Credit Control Configuration Mode Command* chapter in the *Command Line Interface Reference*.

Enhancement to OCS Failure Reporting for Gy

Feature Description

When Cisco-Event-Trigger-Type AVP is installed by PCRF in CCA-I, CCA-U or in RAR messages with value CREDIT_CONTROL_FAILURE (5), then the Cisco-Event grouped AVP is sent by the P-GW to PCRF in CCR-U message with the exact value of OCS failure code. This trigger is sent only when Gy failure occurs and based on the configuration (Credit-Control-Failure-Handling), the ‘Continue’ action is taken and Gy session moves to Offline state.

In releases prior to the implementation of this enhancement, if a failure code was received from OCS in the range of 3000-3999, then Cisco-CC-Failure-Type was sent with the value 3XXX. Similarly, for error codes in the range of 4000-4999 or 5000-5999, Cisco-CC-Failure-Type was reported as 4XXX or 5XXX respectively. With this enhancement, the exact failure code is reported to the PCRF instead of the range. For example, when the Cisco-Event-Trigger-Type is CREDIT_CONTROL_FAILURE (5) and OCS failure code is 3002 in CCA-U, then in CCR-U towards PCRF Cisco-CC-Failure-Type (as part of grouped AVP Cisco-Event) is sent with a value of 3002.

Backpressure Handling

Diameter base (Diabase) maintains an outbound stream. When an application wants to write a message into a socket, the message handle of those messages are stored in the outbound stream. Only on receiving the response to the corresponding request, the stored message handle is removed from the outbound stream. In order to rate-limit the message transactions based on the responses received from the server, ASR 5500 maintains a limit on the number of messages stored in the outbound stream. This is done using "max-outstanding <>" CLI (default value is 256). If the number of messages created by the application exceeds the max-outstanding limit, diabase sends a 'Backpressure' indication to the application to wait till it receives a decongestion indication from diabase to try again.

On receiving a response from the server, the corresponding request message handle will be removed from the outbound stream, creating a slot for another message to be written by the application. In order to intimate this slot availability, decongestion notification is sent to the registered application. The application in turn loops through all sessions and processes the pending trigger to be sent.

When the application loops through the sessions in the system, it traverse the sessions in a sorted order and checks each session whether it has to send a pending CCR-Initial or CCR-Terminate or CCR-Update. When the first session gets the slot to fill the outbound stream, it writes the message into the stream. Now the slot gets back into filled state, reaching the max-outstanding limit again. So the rest of the sessions will still continue to be in backpressured state.

Backpressured request like Credit-Control-Initial and Credit-Control-Terminate are given higher priority over Credit-Control-Update as they are concerned with the creation or termination of a session. So on top of the decongestion notification, DCCA has some internal timers which periodically try to send the message out. So in case of heavy backpressure condition, the probability of CCR-I or CCR-T being sent out is more than CCR-U.

Gy Backpressure Enhancement

This feature facilitates maintaining a list of DCCA sessions that hit backpressure while creating a message i.e., backpressured list, eliminating the current polling procedure. This will maintain a single queue for all types of messages (CCR-I, CCR-U, CCR-T, CCR-E) that are backpressured. The messages will be sent in FIFO order from the queue.

After processing a session from the backpressure queue DCCA will check for the congestion status of the peer and continue only if the peer has empty slots in the outstanding message queue to accommodate further CCRs.

Releases prior to 16.0, the gateway has a max-outstanding configuration to manage a number of messages that are waiting for response from OCS. When the max-outstanding is configured to a low value, then the frequency to be in congested state is very high.

CPU utilization is very high if the max-outstanding count is low and network is congested.

In 16.0 and later releases, all DCCA sessions associated with the CCR messages that are triggered BACKPRESSURE (when max-outstanding has been reached) will be queued in backpressure list which is maintained per ACS manager instance (credit-control) level.

This list will not have any specific configurable limits on the number of sessions that will be queued in it. This is because there is an inherent limit that is already present which is dependent on the number of subscriber/DCCA sessions.

With this new separate backpressured list, CPU utilization will come down under high backpressure case.

Gy Support for GTP based S2a/S2b

For WiFi integration in P-GW, Gy support is provided for GTP based S2a/S2b in Release 18.0. This implementation is in compliance with standard Rel-11 non-3GPP access spec of 32.399: S5-120748 S5-131017 S5-143090.

As part of this enhancement, the following AVP changes are introduced:

- Added TWAN as a new enum value for Serving-Node-Type AVP
- Added a new Diameter AVP "TWAN-User-Location-Info". This is a grouped AVP and it contains the UE location in a Trusted WLAN Access Network (TWAN): BSSID and SSID of the access point.

The TWAN AVPs will be effective only for 3GPP release 11 and it is added only to the standard Gy dictionary. That is, the TWAN AVP will be included in CCR-I/CCR-U/CCR-T messages only when the CLI command "**diameter update-dictionary-avps 3gpp-rel11**" is configured.

Generating OOC/ROC with Changing Association between Rule and RG

The existing Gy implementation prevents duplicate Out-of-Credit (OOC) / Reallocation of Credit (ROC) report for the same rule to the PCRF. Subscriber throttling with the same rule with different Rating-Group across OOC event does not work. To overcome this, the following implementation is considered:

When a Rating-Group runs out of credit, OOC is sent to all rules that are currently associated with that Rating-Group. This is done irrespective of whether that rule was already OOC'd or not. Similarly, when a Rating-Group gets quota after being in OOC state, a ROC is sent to all rules that are currently associated with that Rating-Group. This is done irrespective of whether that rule was already ROC'd or not.

In releases prior to 18, MSCC's state was previously being maintained at MSCC and rule-level to suppress OOC/ROC events. So if MSCC triggered an OOC/ROC the same was suppressed by the status maintained at the rule-level if the previous event on the rule was the same.

In 18 and later releases, the rule level status bits are no longer used to avoid similar back-to-back OOC/ROC events. Now, the triggering of OOC/ROC events will solely be dependent on the MSCC state and triggers.

Customers might see an increase in OOC/ROC events on Gx if they change the association of the rule and RG or if they use the Override feature.

Static Rulebase for CCR

An APN/subscriber can have a single rulebase applied to it, but allowing a static rulebase configuration to always pass a different or same rulebase to the OCS through CCR messages.

A new CLI command "**charging-rulebase-name** *rulebase_name*" has been introduced under Credit Control (CC) group to override/change the rulebase name present in APN/subscriber template, in the CCR AVP "Charging-Rule-Base-Name". The rulebase value configured in CC group will be sent to OCS via CCR. If this CLI command is not configured, then the rulebase obtained from APN/subscriber template will be sent to OCS.

The configured value of rulebase under CC group is sent in all CCR (I/U/T) messages. This implies that any change in rulebase value in CC group during mid-session gets reflected in the next CCR message.

This feature, when activated with the CLI command, reduces the complication involved in configuration of services like adding and removing services per enterprise on the OCS system.

CC based Selective Gy Session Control

This section describes the overview and implementation of the Selective Gy Session Control feature based on Charging Characteristics (CC) profile of the subscriber.

This section discusses the following topics for this feature:

Feature Description

The functionality that allows users to configure certain Charging Characteristics (CC) values as prepaid/postpaid is available for GGSN service. In Release 17, this functionality is extended to P-GW service.

To enable/disable Gy session based on the CC value received, the APN configuration is extended so that additional credit-control-groups/prepaid prohibited value can be configured for each of the CC values.

The **cc profile** *cc-profile-index* **prepaid prohibited** CLI command is used to configure the CC values to disable Credit-Control based charging. The P-GW/GGSN/SAEGW service subscriber sessions using this APN, can use this configuration to stop the triggering of Gy messages towards the OCS.

The UE provides the charging characteristics value and the active subscriber is connected through an APN. The CC index mapping is done for a corresponding CC group/prepaid prohibited value configured under the APN. Depending on the match, the Gy session is enabled or disabled towards the OCS.

The Session controller stores/updates the APN configuration in the AAA manager. During the session setup, the session manager fills the CC value received in session authenticate request, and sends it to AAA manager. The AAA manager matches this against the locally stored APN configuration, and selects the desired credit-control-group/prepaid-prohibited configuration for the session. Then the session manager passes this credit-control-group/prepaid-prohibited information received from the AAA manager to ACS manager.

When the local authentication (session setup request) is done, the credit-control group with the matching charging characteristic is selected and used. If there is no matching charging characteristic configuration found for the credit-control group selection, then the default credit-control group for the APN is selected.

When a particular CC is configured as postpaid, any session with this CC does not trigger Gy connection. Any change in the CC during the lifetime of session is ignored.

The CC based Gy Session Controlling feature is applicable only for the CC value received via GTP-Auth-Request, and during the session establishment. The CC value updated via AAA/PCRF after the session setup will not cause any change in already selected credit-control group. Once the credit-control group is selected after session setup, this feature is not applicable.

Diamter Error Code and Counters

SaMOG supports Diameter error code counters for all transactions and diameter interfaces on SaMOG (Web-auth) services through P-GW LBO module on various StarOS platforms ASR5500/ASR5700.

The following set of result code specific counters are available for the responses received from the OCS (Online Charging System), on Gy interface. DCCA (Diameter Credit Control Application) is the protocol used on the Gy interface.

Table 16: Result Code Specific Counters

Error Category	Result Code	Result Code Value
Transient Failures [4XXX]	DIAMETER_END_USER_SERVICE_DENIED	4010
	DIAMETER_CREDIT_LIMIT_REACHED	4012
Permanent Failures [5XXX]	DIAMETER_RATING_FAILED	5031

Relationships to Other Features

This feature can also be used when the CC profile configuration is enabled through the GGSN service. When the CC profile is configured under APN service and GGSN service, the prepaid prohibited configuration for the matching CC profile is applied irrespective of the services.

Limitations

The following are the limitations of this feature:

- One charging characteristic value can be mapped to only one credit-control-group/prepaid-prohibited configuration within one APN.
- The charging-characteristic based OCS selection is possible only during the session-setup. Once the credit-control-group is selected (after session setup), this feature is not applicable.

Configuring CC based Selective Gy Session Control

The following sections provide the configuration commands to configure the Gy Session Control feature based on the CC profile of the subscriber.

Configuring CC Value

The following commands are used to configure Charging Characteristic values as postpaid/prepaid to disable/enable Gy session towards the OCS.

```
configure
  context context_name
    apn apn_name
      cc-profile { cc_profile_index | any } { prepaid-prohibited |
credit-control-group cc_group_name }
      end
```

Notes:

- *cc_profile_index*: Specifies the CC profile index. *cc_profile_index* must be an integer from 0 through 15.
- **any**: This keyword is applicable for any non-overridden cc-profile index. This keyword has the least priority over specific configuration for a CC profile value. So, configuring **any** keyword will not override other specific configurations under APN.
- **prepaid-prohibited**: Disables prepaid Gy session for the configured profile index.
- *cc_group_name*: Specifies name of the credit control group as an alphanumeric string of 1 through 63 characters.
- **no cc-profile** *cc_profile_index*: This command falls back to "any" cc-profile behavior irrespective of the CC profile index value configured.

Verifying the Selective Gy Session Control Configuration

Use the following command in Exec mode to display/verify the configuration of Selective Gy Session Control feature.

```
show configuration
```

Monitoring and Troubleshooting the Selective Gy Session Control Feature

This section provides information regarding show commands and/or their outputs in support of the Selective Gy Session Control feature.

show active-charging sessions

The "Credit-Control" field that appears as part of the **show active-charging sessions [callid | imsi | msisdn]** command output enables the user to determine the credit control state as "On" for online charging enabled session or "Off" for prepaid prohibited session and monitor the subscriber session.

Credit-Control Group in Rulebase Configuration

This section describes the overview and implementation of the Credit-Control (CC) Group Selection based on the rulebase of the subscriber.

This section discusses the following topics for this feature:

Feature Description

This feature is introduced to customize the behavior for different types of subscribers in the Assume Positive scenario. This customization is made by enabling the users to specify a desired Credit-Control (CC) group based on the rulebase dynamically selected by PCRF.

Typically, the behavior for Assume Positive is configured within the CC group. In releases prior to 20, there were options to choose the CC group through APN/subscriber-profiles, IMSA, or AAA configurations. In this release, the CC group selection functionality is extended to rulebase configuration.

This feature is explicitly required in scenarios where IMSA was not used, AAA server could not send CC group during authentication, and only a single APN/subscriber-profile was used for all the subscribers. In such situations, this feature targets to provide a premium CC group within rulebase to enable premium treatment to subscribers based on their types.

This feature introduces a new configurable option inside the rulebase configuration, so that the users can specify the desired CC group whenever the rulebase is selected during the subscriber session setup. This configured CC group overrides or has a higher priority than the CC group configured within the subscriber profile/APN. If the AAA or PCRF server sends the CC-Group AVP, the CC group value defined through the AVP overrides the rulebase configured CC group.

When this feature is enabled, the configuration allows specifying an association between the rulebase name and the CC group so that when a premium subscriber connects, a premium rulebase and a premium CC group are selected.

Important Mid-session configuration change will not impact the existing subscribers in the system. This configuration change will be effected only to the new sessions.

Implementing this new configuration option enables different types of Assume-Positive behavior for subscribers based on the available quota. This results in achieving preferential treatment for premium customers.

The precedence order for selection of the CC group is defined as:

- PCRF provided CC group

- AAA provided CC group
- Rulebase configured CC group
- Subscriber Profile/APN selected CC group
- Default Credit-Control group

Important This feature should not be used when there is an option for AAA server to send the CC group during authentication process. If during the authentication, AAA server sends a CC group, and the rulebase selected has a CC group defined within, then the rulebase defined CC group is selected for the session.

Limitations

There are no limitations or restrictions with this feature. However, it is important to keep in mind the precedence order for CC group selection.

Configuring Credit-Control Group in Rulebase

The following sections provide the configuration commands to configure the Credit-Control Group based on the rulebase of the subscriber.

Defining Credit-Control Group

The following commands are used to configure a desired Credit-Control group name when using the rulebase selected by PCRF.

```
configure
require active-charging
active-charging service service_name
   rulebase rulebase_name
      credit-control-group cc_group_name
      end
```

- *cc_group_name*: Specifies name of the credit control group as an alphanumeric string of 1 through 63 characters.
- **no credit-control-group**: Removes the previously configured CC group from the rulebase configuration. This is the default setting.
- This CLI configuration is applicable only during the session setup. Mid-session change in the CC group is not allowed.
- This is an optional CLI configuration, and used only when customized Assume Positive behavior is required for subscribers.
- If this CLI command is configured, the selection of the CC group will be based on the precedence order. That is, the rulebase defined CC group has higher precedence over the CC group value specified in the Subscriber/APN profile.
- If the CC group configuration is not present in the rulebase, the default subscriber/APN profile configuration is applied.

Verifying the Credit-Control Group Configuration

Use the following command in Exec mode to display/verify the configuration of CC group in rulebase.

```
show configuration verbose
```

Monitoring and Troubleshooting the CC-Group Selection in Rulebase

This section provides information regarding show commands and/or their outputs in support of this feature.

show active-charging sessions full

The output of this show CLI command displays the selected credit-control-group for the session. The output details are useful in verifying and troubleshooting the issues with this feature.

show configuration errors

This show CLI will list an error if the credit-control group that is configured inside the rulebase is not defined.

show configuration verbose

This command will show the "credit-control-group" option specified for the rulebase. For troubleshooting purpose, capture the output of **show configuration verbose** and **show subscribers full** along with the **monitor-protocol** output containing "Radius Access-Accept".

Combined CCR-U Triggering for QoS Change Scenarios

In release 20, the number of CCR-Us sent to the OCS is controlled for QoS change scenarios in P-GW call. This new behavior is introduced in the system to easily handle the issues with Transactions Per Second (TPS) on OCS.

In releases prior to 20, for a change in the default EPS bearer QoS and APN AMBR received from PCRF for LTE or S2b WiFi calls, P-GW used to send two separate CCR-Us to OCS through Gy interface, one each for QoS change and AMBR change. In 20 and later releases, when default EPS bearer QoS and APN AMBR values are changed, P-GW sends update request to access side to change default bearer and APN AMBR in a single message. P-GW will apply APN AMBR and default bearer QoS accordingly and will send only one CCR-U on Gy for this change condition.

Important This behavior change is applicable only to P-GW calls. This change has no impact to the Rf/CDR records, and GGSN/P-GW eHRPD calls.

Also, note that this behavior is not applicable for split TFT case (QoS + APN AMBR + TFT) wherein multiple Update Bearer Requests are sent towards the access side.

Re-activating Offline Gy Session after Failure

This section describes the feature to re-enable Offline Gy session on detecting failure at Diameter Credit Control Application.

This section includes the following topics:

Feature Description

With this feature, a mechanism to re-enable the Offline Gy session back to Online charging, based on indication from PCRF is introduced in this release. Upon receiving the Online AVP from PCRF, the gateway will establish the Gy session.

In previous releases, there was no provision to activate Gy once the session was marked as Offline. On detecting failure at Diameter Credit Control Application, the configured Credit Control Failure Handling (CCFH) action would be taken. Once the Gy session has taken the CCFH Continue action, the subscriber session could not be retried/re-enabled.

The Online AVP in the Charging-Rule-Definition is considered as the trigger/indication from PCRF to enable the Offline Gy session, after the CCFH Continue action been taken. The Online AVP at the command level from PCRF will not be considered as a trigger to enable the Offline Gy session. As per 3GPP 29.212 (release 12.12.0), the Online AVP (1009) is an optional AVP inside the Charging-Rule-Definition grouped AVP (1003).

Limitations and Restrictions

This section lists the limitations and configuration restrictions with this feature:

- This feature is limited only to Volume Quota mechanism. Special handling is not done for Quota-Validity-Time (QVT) and Quota-Hold-Time (QHT) timers. When the Gy session goes offline and comes back again, these timers are not started. The timers will be started only when the next CCA-U provides the information from OCS.
- When the Gy session is marked Online, CDR closure is not required and this is handled by the billing system.
- This feature is not extended to the event-based credit-control sessions.
- When the CCFH action is taken due to MSCC level failure, the existing behavior is retained and the following behavior is observed:
  - CCFH Continue – Continue the category (MSCC) without charging at Gy and this is applicable to the MSCC (not to the entire session). The MSCC state in the output of the **show active-charging sessions full** command will display "No Charge".
  - CCFH Terminate/Retry-and-Terminate – The bearer gets terminated.
- When the Result-Code 4011 (DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE) is received at MSCC level, the category is marked Free-of-Charge and no further accounting for this category is done. When this result code is received at command level, the Gy session is made Offline. The Offline Gy session can be made Online again using the Online AVP from PCRF and the accounting will resume normally (CCR-U will be seen at OCS for this session).
- When CCFH Continue is configured and CCR-I failure occurs, the following behavior is observed:
  - Diabase Error – When diabase error (TCP connection down) occurs, the Gy session is marked Offline and the session-state is maintained (session-ID created). When re-enabling the Gy session, a new CCR-I is sent immediately (without waiting for data).
  - Response Timeout – When the response timeout happens, if the CCR-I is sent at session-setup and the session-setup timeout happens before response-timeout, then the bearer itself will be terminated. The **diameter send-crri traffic-start** configuration can be used optionally so that the CCR-I timeout does not affect the bearer creation.

- When the Gy session goes Offline due to CCR-I response timeout and the Gy session is marked Online, the same Session-ID will be used.
- If the Gy session went offline due to CCR-I error response, the session-information is deleted (next session-ID used will be different).

- In case of rule-movement across bearers (LTE to WiFi or vice-versa) where the Online rule is moved/associated to an existing bearer, the status of the Gy session is not changed.
- The trigger for marking the Offline Gy Session to Online is only based on the Online AVP received from the PCRF in the Charging-Rule-Definition.

Configuring Offline Gy Session after Failure

The following section provides the configuration commands to re-enable the offline Gy session.

Re-enabling Offline Gy Session

Use the following configuration to re-enable offline Gy session after failure.

```
configure
  active-charging service service_name
    credit-control
      [ no ] offline-session re-enable
      end
```

Notes:

- When **offline-session re-enable** is configured and the PCRF installs/modifies a rule with "Online" AVP value set to 1, then the Offline DCCA will be marked Online.
- The default configuration is **no offline-session re-enable**. This feature is disabled by default and when disabled only the **show configuration verbose** command will display this configuration.

Verifying the Configuration

Use the following command to verify the offline/online state transition timestamp:

```
show active-charging sessions full
```

Monitoring and Troubleshooting the Offline Gy Session after Failure

This section provides information regarding show commands and/or their outputs in support of this feature.

The following operations should be performed to troubleshoot any failure related to this feature:

- The CLI output of the **show active-charging sessions full** command can be verified. The "Last State Change Time" field indicates the timestamps at which a session went Offline and came back Online.
- The messages from **monitor subscriber next-call** command can be enabled with "verbosity 3" to analyze the message exchanges happening for the subscriber.
- The "acsmgr" and "debug" level logs can be enabled for further debugging.

show active-charging sessions full

The following new fields are added to the output of this command to display the state transition timestamp:

- Last State Change Time:
  - Offline/Online – The Offline timestamp is updated when the Gy session goes Offline. The Online timestamp is updated when the session is back Online.

Suppress AVPs

This feature adds enhancement to the *Support MVNO Information in Gx, Gy and CDRs* feature.

Feature Description

This feature adds enhancement to the *Support MVNO Information in Gx, Gy and CDRs* feature. SAEGW sends MVNO-Reseller-ID and MVNO-Subclass-ID AVPs in the Gy messages towards the OCS and CDR, whenever these AVPs are received by SAEGW from the PCRF.

With this enhancement, this behavior is now CLI controlled and a new CLI command has been introduced to suppress the AVPs being sent in the Gy interface.

Old Behavior: Reseller-id and subclass-id AVPs were send in Gy when the same were received from PCRF for the ATT dictionary.

New Behavior: New CLI command **suppress_avp**has been added which allows to suppress the Reseller-id and subclass-id AVPs.

Command Changes

suppress_avp

New CLI command has been added to the Credit Control Group configuration mode to suppress the AVPs. Configuring this CLI command would suppress the MVNO-subclass-id and MVNO-Reseller-Id AVPs.

```
configure
  active-charging service <acs_service_name>
    credit-control group <group_name>
      diameter suppress-avp reseller-id subclass-id
      [ no | default ] diameter suppress-avp reseller-id subclass-id
  end
```

Notes:

- **no:** Disables AVP suppression. Whenever PCRF sends the MVNO-subclassid and MVNO-Reseller-id AVPs in the Gx interface, the same is sent in the Gy message.
- **default:** Sets the default configuration. AVPs are not suppressed by default. Whenever PCRF sends the MVNO-subclassid and MVNO-Reseller-id AVPs in the Gx interface, the same is sent in the Gy message.
- **suppress-avp:** Suppresses both MVNO-subclassid and MVNO-Reseller-id AVPs.
- **reseller-id:** Supresses the MVNO-Reseller-Id AVP.
- **subclass-id:** Supresses the MVNO-Sub-Class-Id AVP.

Performance Indicator Changes

show configuration

This command has been modified to display the following output:

```
credit-control group default
      diameter origin endpoint sundar
      diameter peer-select peer minid1 secondary-peer minid2
      diameter session failover
      diameter dictionary dcca-custom32
      failure-handling initial-request continue
      failure-handling update-request continue
      diameter dynamic-rules request-quota on-traffic-match
      diameter suppress-avp reseller-id subclass-id
```

Configuring Gy Interface Support

To configure Gy interface support:

Step 1 Configure the core network service as described in this Administration Guide.

Step 2 Configure Gy interface support as described in the sections Configuring GGSN / P-GW / IPSG Gy Interface Support, on page 239 and Configuring HA / PDSN Gy Interface Support, on page 240.

Step 3 Configure Event-based Gy support as described in Configuring PLMN and Time Zone Reporting, on page 241.

Step 4 *Optional.* Configure OCS Unreachable Failure Handling Feature or Assume Positive for Gy Feature as described in Configuring Server Unreachable Feature, on page 242.

Step 5 *Optional.* Configure Static Rulebase for CCR as described in Configuring Static Rulebase for CCR, on page 243.

Step 6 *Optional.* Configure Gy for GTP based S2a/S2b as described in Configuring Gy for GTP based S2a/S2b, on page 244.

Step 7 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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.

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 *System Administration Guide*.
- For more information on configuring ECS ruledefs, refer to the *ACS Ruledef Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- For more information on configuring ECS charging actions, refer to the *ACS Charging Action Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- For more information on configuring ECS rulebases, refer to the *ACS Rulebase Configuration Mode Commands* chapter in the *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 *System Administration Guide*.
- For more information on configuring ECS ruledefs, refer to the *ACS Ruledef Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- For more information on configuring ECS charging actions, refer to the *ACS Charging Action Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- For more information on configuring ECS rulebases, refer to the *ACS Rulebase Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

Configuring PLMN and Time Zone Reporting

PLMN and Time Zone Reporting feature requires a credit-control group to be defined in the APN or subscriber configuration or there must be a default credit-control group configured. The following CLI commands are available to enable/disable PLMN and Time Zone Reporting feature.

To enable PLMN and Time Zone Reporting through subscriber-template, use the following configuration:

```
configure
     context <context_name>
          subscriber name <subscriber_name>
               dns primary <primary_ipaddress>
               dns secondary <secondary_ipaddress>
               ip access-group test in
               ip access-group test out
               ip context-name <context_name>
               credit-control-client event-based-charging
               active-charging rulebase <rulebase_name>
               exit
               end
```

Notes:

- The **credit-control-client event-based-charging** command should be used to enable PLMN and Time Zone Reporting.

  For more information on configuring PLMN and Time Zone Reporting feature, refer to the *Command Line Interface Reference*.

To enable PLMN and Time Zone Reporting through APN template, use the following configuration:

```
configure
     context <context_name>
          apn <apn_name>
               selection-mode sent-by-ms
               accounting-mode none
               ip access-group test in
               ip access-group test out
               ip context-name <context_name>
               ip address pool name<pool_name>
               credit-control-client event-based-charging
               active-charging rulebase <rulebase_name>
               exit
               end
```

Rest of the parameters needed for Event-based Gy such as dictionary, endpoint will be picked from the credit-control group.

In a scenario where the triggers are configured through the CLI command and another set of triggers are also received from Gx, then the triggers from Gx will have a higher priority.

Configuring Server Unreachable Feature

The Server Unreachable feature requires a failure handling behavior to be defined in the Diameter Credit Control configuration. The following CLI commands are available to enable/disable OCS Unreachable Failure Handling feature.

To enable OCS Unreachable Failure Handling feature, use the following configuration:

```
configure
require active-charging
```

```
          active-charging service <service_name>
               credit-control
                    servers-unreachable { initial-request | update-request
 } { continue | terminate }  [ { after-interim-volume <bytes> |
after-interim-time <seconds> } +   server-retries <retry_count> ]
                  servers-unreachable behavior-triggers { initial-request
 | update-request } transport-failure [ response-timeout | tx-expiry ]
                   servers-unreachable behavior-triggers initial-request
 { result-code { any-error | result-code [ to end-result-code ] } }
                   servers-unreachable behavior-triggers update-request
{ result-code { any-error | result-code [ to end-result-code ] } }
                  end
```

Important After you configure **configure**, **require active-charging** , **active-charging service** <*service_name*>, and **credit-control** CLI commands, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Notes:

- This CLI command "**servers-unreachable { initial-request | update-request } { continue | terminate } [{ after-interim-volume ...**" allows configuring interim-volume and interim-time in the following ways:
  - after-interim-volume <bytes> alone followed by server-retries.
  - after-interim-time <secs> alone followed by server-retries.
  - after-interim-volume <bytes> after-interim-time <secs> followed by server-retries.
- This CLI command "**servers-unreachable behavior-triggers**" is used to trigger the servers-unreachable failure handling at either Tx expiry or Response timeout (This CLI is similar to retry-after-tx-expiry in "**failure-handling update-request continue retry-after-tx-expiry**" command.).
- This CLI command "**servers-unreachable behavior-triggers initial-request { result-code { any-error | result-code [to end-result-code] } }**" is used to trigger the servers-unreachable failure handling based on the configured Diameter error result codes.

For more information on configuring this feature, refer to the *Command Line Interface Reference*.

Configuring Static Rulebase for CCR

To allow static configuration of rulebase name to be passed to OCS via CCR message, use the following configuration:

```
configure
    require active-charging
    active-charging service service_name
         credit-control group  ccgroup_name
              charging-rulebase-name rulebase_name
              no charging-rulebase-name
              end
```

Important After you configure **configure**, **require active-charging**, **active-charging service** *service_name*, and **credit-control group** *ccgroup_name* CLI commands, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Notes:

- By default, the rulebase obtained from APN/subscriber template will be sent to OCS through the CCR message.

For more information on configuring this feature, refer to the *Command Line Interface Reference*.

Configuring Gy for GTP based S2a/S2b

To provide Gy Support for WiFi integration in P-GW for GTP based S2a/S2b, use the following configuration:

```
configure
    require active-charging
    active-charging service service_name
         credit-control group  ccgroup_name
              diameter update-dictionary-avps 3gpp-rel11
              [  default | no ] diameter update-dictionary-avps
              end
```

Notes:

- **3gpp-rel11**: Provides support for 3GPP Rel.11 specific AVPs in the standard Gy dictionary.

Gathering Statistics

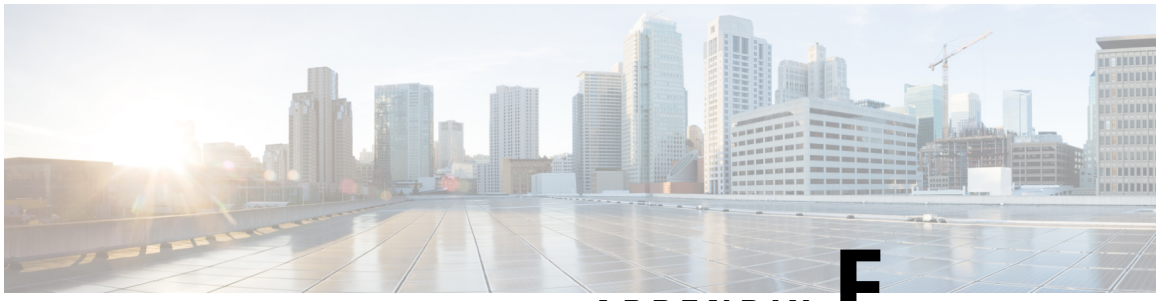
This section explains how to gather Gy related statistics and configuration information.

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**
Detailed information for the Active Charging Service (ACS)	**show active-charging service all**
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**

Statistics/Information	Action to perform
States of the Credit Control application's sessions, DCCA.	**show active-charging credit-control session-states [rulebase** <*rulebase_name*> **] [content-id** <*content_id*> **]**

Gy Interface Support



APPENDIX F

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.

The following products currently support ICAP interface functionality:

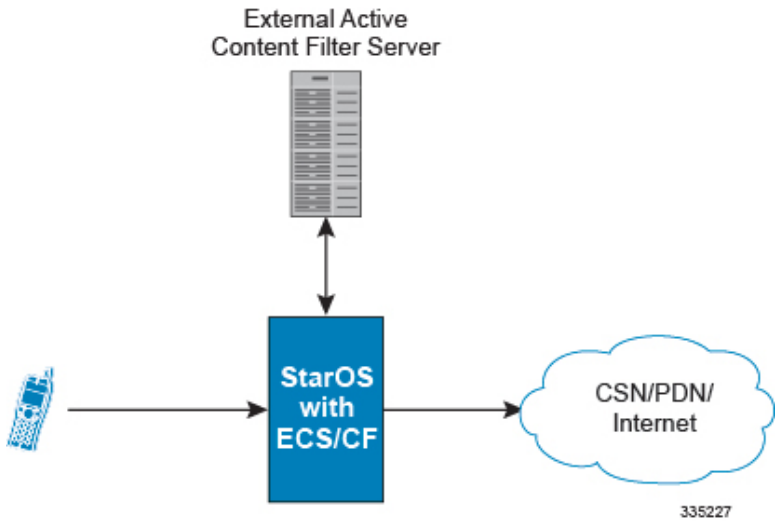
- GGSN
- P-GW

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 19: 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. WAP and HTTP traffic is content filtered over the ICAP interface. RTSP traffic that contains adult content can also be content filtered on the ICAP interface. Only the RTSP Request packets will be considered for content filtering over the ICAP interface.

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 must be redirected.
- Deny-response code 200 for RTSP requests is not supported. Only 403 "Forbidden" deny-response code will be supported.

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

Supported Networks and Platforms

This feature supports the Cisco ASR 5500 platform for the core network services configured on the system.

For additional platform information, refer to the appropriate *System Administration Guide* and/or contact your Cisco account representative.

License Requirements

External Content Filtering Server support through Internet Content Adaptation Protocol (ICAP) interface is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements.

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

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.
- RTSP:

  The following scenarios describe the failure actions where an RTSP request is received from the client. If ICAP is enabled, then the request goes to the ICAP server for content filtering.
  - Allow: If the failure action configured is "allow", the RTSP request packet is sent out after applying the appropriate disposition action. Here, the flow remains the same as in the case if the ICAP response received is 200 OK.
  - Content Insert: If the failure action configured is "content-insertion <string of size 1 to 128>", then this failure action for RTSP request will not be supported. Instead the failure action "Discard" for such an RTSP request will be supported.
  - Redirect-URL: If the failure action configured is "redirect-url <string of size 1 to 128>", then a TCP FIN_ACK packet with an RTSP "302 Moved Temporarily" response header is inserted towards the client containing the said URL for redirection. A TCP RST packet is inserted towards the server. The underlying TCP connection is thus closed. If the RTSP client wants to retry to the redirected URL, the opening of a new TCP connection must be initiated.
  - Discard: If the failure action configured is "discard", then the RTSP request packet received from the client is quietly discarded and no notification is sent to the client.
  - Terminate flow: If the failure action configured is "terminate-flow", then the TCP connection is torn down by injecting a TCP FIN-ACK towards the client and a RST packet towards the server. However, no notification will be sent to the RTSP client and the server regarding this flow termination.

ICAP Client Communication with RFC 3507 compliance

The ICAP Content Filtering solution is extended to support ICAP client communication with ICAP server on Cisco ASR 5500 P-GW and HA in compliance with RFC 3507 - Internet Content Adaptation Protocol (ICAP). Only HTTP Request modification and partial enhancement of error codes per RFC 3507 is addressed in this release. The ICAP client running on P-GW/HA communicates with external ICAP server over ICAP protocol. If content filtering is enabled for a subscriber, all HTTP GET requests from that subscriber are validated by

the content filtering server (ICAP server), and is allowed, denied or redirected depending on the content categorization request.

Content-Filtering can be enabled for subscribers either through Override Control (OC) feature for predefined and static rules, or L7 Dynamic Rule Activation feature. A configurable option is added in the Content Filtering Server Group Configuration Mode to configure ICAP header that includes two parameters - Subscriber number information and CIPA (Children's Internet Protection Act) category.

Important Override Control and L7 Dynamic Rule Activation are license-controlled features. A valid feature license must be installed prior to configuring these features. Contact your Cisco account representative for more information.

- Subscriber Number: The "Subscription ID" AVP is sent from gateway to PCRF in CCR message. The AVP values are received to the gateway from HSS. The gateway does not receive this AVP in CCI-A message.
- CIPA category: The category string will be provided by PCRF and is included as an extension header in ICAP request modification message. The AVP will be received from PCRF in CCA-I or RAR.

Dictionary and AVP Support

A new Content Filtering (CF) dictionary "custom4" is introduced and the following new AVPs are added to r8-gx-standard and custom4 dictionaries.

- Override-Content-Filtering-State: This attribute carries information about Content Filtering status (CF state) of rules or charging-action. This AVP is used for overriding the content-filtering status of static and predefined rules. This attribute is included in the Override-Control grouped AVP.
- CIPA: This attribute contains the Children's Internet Protection Act (CIPA) category string value that is treated as an ICAP plan identifier. This identifier helps ICAP server in locating the correct Content Filtering plan i.e. CIPA category based on which the packet is processed.

  This attribute value is received from PCRF over Gx interface and is included in ICAP header while sending ICAP request.
- L7-Content-Filtering-State: This attribute carries information about Content Filtering status (CF state) of L7 rules. This attribute indicates whether or not the ICAP functionality is enabled or disabled for L7 charging rule definition received for installation from PCRF. Based on this attribute value, the traffic matching to the dynamic rule is sent to ICAP server.

  This attribute is included in the L7-Application-Description grouped AVP for L7 rule processing. This is applicable only for HTTP protocol.

Important CIPA and flags for controlling content filtering via OC and L7 Dynamic Rules features is applicable only for r8-gx-standard dictionary.

In addition to the new AVP support, L7-Field AVP in the L7-Application-Description grouped AVP is encoded to additionally accept ANY-MATCH as the input. The current framework does not support the existing field "vlan-id" in Override-Control, which is present in charging action. Hence, the Override-Content-Filtering-State AVP replaces Override-VLAN-ID to support OC.

When subscriber initiates create session request, P-GW/HA sends CCR-I message to PCRF to obtain subscriber profile. PCRF responds with CCA-I message that contains CIPA and OC information if ICAP functionality is enabled for this subscriber.

In the case of L7 dynamic rules, the Content-Filtering capability is enabled by sending L7-Content-Filtering-State AVP in L7-Application-Description grouped AVP. At least one L7 filter should be present when L7-Content-Filtering-State is received for the dynamic rule. If L7-Content-Filtering-state AVP is sent along with L7 filter information AVP, then the Content-Filtering state will not be considered. Hence, the filter received with L7-Content-Filtering-State will not be processed and the L7 rule will be discarded.

In the case of Override Control, when content filtering is enabled for subscriber, PCRF sends ICAP flag through Override-Control AVP. This AVP overwrites charging action to enable ICAP feature for that subscriber.

Refer to the *AAA Interface Administration and Reference* for more information on the supported AVPs.

Limitations

The limitations for this feature are listed below:

- Only IPv4 addressing scheme is supported.
- ICAP content filtering is applicable only for HTTP traffic. HTTPS traffic is not supported by ICAP client.
- Accelerated path will not be supported for this feature.

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 *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 Creating ICAP Server Group and Address Binding, on page 253.

Step 2 Specify the active content filtering server (ICAP server) IP addresses and configure other parameters for ICAP server group by applying the example configuration in Configuring ICAP Server and Other Parameters, on page 253.

Step 3 Configure the content filtering mode to external content filtering server group mode in ECS rule base by applying the example configuration in Configuring ECS Rulebase for ICAP Server Group, on page 254.

Step 4 Configure the charging action to forward HTTP/RTSP/WAP GET request to external content filtering servers on ICAP interface in Active Charging Configuration mode by applying the example configuration in Configuring Charging Action for ICAP Server Group, on page 254.

Step 5 Verify your ICAP interface and external content filtering server group configuration by following the steps in Verifying the ICAP Server Group Configuration, on page 255.

Step 6 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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> ] [ standby ]
         connection retry-timeout <retry_timeout>
         deny-message <msg_string>
         dictionary { custom1 | custom2 | custom3 | custom4 | standard }
        failure-action { allow | content-insertion <content_string> | discard
 | redirect-url <url> | terminate-flow }
         header extension options { cipa-category cipa_category_name |
subscriber-number subscriber_num_name } +
         response-timeout <timeout>
         end
```

Notes:

- In 8.1 and later releases, a maximum of five ICAP servers can be configured per Content Filtering Server Group. In release 8.0, only one ICAP Server can be configured per Content Filtering Server Group.
- The **standby** keyword can be used to configure the ICAP server as standby. A maximum of ten active and standby ICAP servers per Content Filtering Server Group can be configured. The active and standby servers under the same server group can be configured to work in active-standby mode.
- 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.

- The **custom4** dictionary is a custom-defined dictionary that specifies user-defined information in the ICAP request message. The ICAP request message includes subscriber number and CIPA category values.

  When **custom4** dictionary is configured, ICAP requests are formed as part of ICAP RFC 3507 request mode request. If any other dictionary is configured, the earlier implementation of ICAP client will not be partial RFC compliant.

- The **header extension options** command configures ICAP header parameters - subscriber number and CIPA category.

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

Important After you configure **configure**, **require active-charging [optimized-mode]**, **active-charging service** *<acs_svc_name>* **[-noconfirm]**, and **rulebase** CLI commands, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

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 ]
         [ no ] content-filtering processing server-group
         end
```

Notes:

- If the content-filtering flag supplied by charging action is required to configure the Override Control feature, then the **no content-filtering processing** command must be configured. This will ensure overriding content-filtering processing to be enabled or disabled through the Override Control feature.

Verifying the ICAP Server Group Configuration

This section explains how to display and review the configurations after saving them in a .cfg file 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
    Header Extension Options:            subscriber-number i-sub
    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