HA Administration Guide, StarOS Release 21.15

First Published: 2019-08-29

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

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

The Home Agent(HA) is a StarOS application that runs on Cisco® ASR 5500 and virtualized platforms. The Cisco Mobile Wireless Home Agent (HA) works in conjunction with a Foreign Agent (FA) and mobile node to provide an efficient Mobile IP solution.

- Conventions Used, on page xvii
- Supported Documents and Resources, on page xix
- Contacting Customer Support , on page xx

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.
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.

Typeface Conventions	Description
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.
|	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 following common documents are available:

- *AAA Interface Administration and Reference*
- *Command Line Interface Reference*
- *GTPP Interface Administration and Reference*
- *Installation Guide* (platform dependant)
- *Release Change Reference*
- *SNMP MIB Reference*
- *Statistics and Counters Reference*
- *System Administration Guide* (platform dependant)
- *Thresholding Configuration Guide*

Related Product Documentation

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

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

- *ADC Administration Guide*
- *CF Administration Guide*
- *ECS Administration Guide*
- *ePDG Administration Guide*
- *GGSN Administration Guide*
- *HSGW Administration Guide*
- *IPSec Reference*
- *MME Administration Guide*
- *NAT Administration Guide*
- *PDSN Administration Guide*
- *PSF Administration Guide*
- *P-GW Administration Guide*
- *SAEGW Administration Guide*
- *SaMOG Administration Guide*
- *SecGW Administration Guide*
- *SGSN Administration Guide*
- *S-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

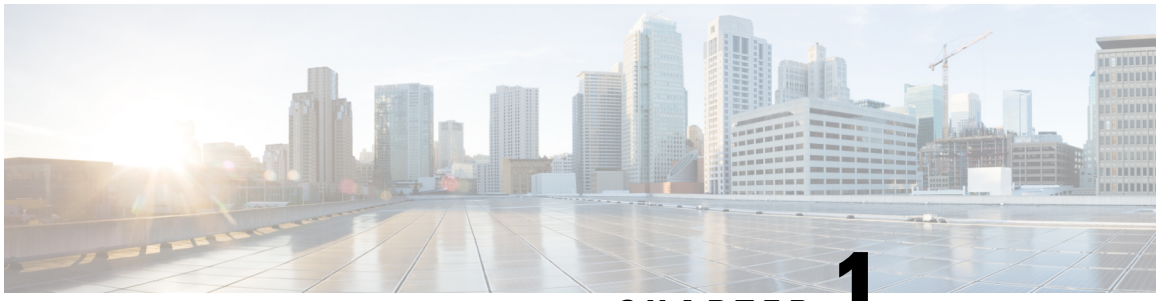
Use the following path selections to access the HA documentation:

Products > Wireless > Mobile Internet> Network Functions > Cisco PDSN/HA Packet Data Serving Node and Home Agent

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

HA Overview

The Home Agent (HA) allows mobile nodes to be reached, or served, by their home network through its home address even when the mobile node is not attached to its home network. The HA performs this function through interaction with a Foreign Agent (FA) that the mobile node is communicating with using the Mobile IP (MIP) standard. Such transactions are performed through the use of virtual private networks that create MIP tunnels between the HA and FA.

When functioning as an HA, the system can either be located within the carrier\'s 3G network or in an external enterprise or ISP network. Regardless, the FA terminates the mobile subscriber\'s PPP session, and then routes data to and from the appropriate HA on behalf of the subscriber.

HA supports IPSec features that you may wish to include in your configuration. Refer to the *StarOS IP Security (IPSec) Reference Guide* for additional information.

This chapter includes the following sections:

Product Specifications

The following application and line cards are required to support CDMA2000 wireless data services on the system:

Hardware Requirements

Qualified Platforms

HA 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.

Operating System Requirements

The HA is available for all Cisco ASR 5500 platform running StarOS Release 12.2 or later. It is also available for ST16 StarOS Release 7.0 or later.

MPLS Forwarding with LDP

Multi Protocol Label Switching (MPLS) is an operating scheme or a mechanism that is used to speed up the flow of traffic on a network by making better use of available network paths. It works with the routing protocols like BGP and OSPF and therefore it is not a routing protocol.

It generates a fixed-length label to attach or bind with the IP packet's header to control the flow and destination of data. The binding of the labels to the IP packets is done by the label distribution protocol (LDP). All the packets in a forwarding equivalence class (FEC) are forwarded by a label-switching router (LSR) which is also called an MPLS node. The LSR uses the LDP in order to signal its forwarding neighbors and distribute its labels for establishing a labelswitching path (LSP).

In order to support the increasing number of corporate APNs which have a number of different addressing models and requirements, MPLS is deployed to fulfill at least following two requirements:

- The corporate APN traffic must remain segregated from other APNs for security reasons.
- Overlapping of IP addresses in different APNs.

When deployed, MPLS backbone automatically negotiates the routes using the labels binded with the IP packets. Cisco GGSN as an LSR learns the default route from the connected provider edge (PE) while the PE populates its routing table with the routes provided by the GGSN.

Features and Functionality - Inline Service Support

This section describes the features and functions of inline services supported on the HA. These services require additional licenses to implement the functionality.

Content Filtering

The Cisco HA offers two variants of network-controlled content filtering / parental control services. Each approach leverages the native DPI capabilities of the platform to detect and filter events of interest from mobile subscribers based on HTTP URL or WAP/MMS URI requests:

- Integrated Content Filtering: A turnkey solution featuring a policy enforcement point and category based rating database on the Cisco HA. An offboard AAA or PCRF provides the per-subscriber content filtering information as subscriber sessions are established. The content filtering service uses DPI to extract URL's or URI's in HTTP request messages and compares them against a static rating database to determine the category match. The provisioned policy determines whether individual subscribers are entitled to view the content.
- Content Filtering ICAP Interface: This solution is appropriate for mobile operators with existing installations of Active Content Filtering external servers. The service continues to harness the DPI functions of the ASR 5500 platform to extract events of interest. However in this case, the extracted requests are transferred via the Integrated Content Adaptation Protocol (ICAP) with subscriber identification information to the external ACF server which provides the category rating database and content decision functions.

Integrated Adult Content Filter

Provides a value-added service to prevent unintended viewing of objectionable content that exploits underage children. Content Filtering offers mobile operators a way to increase data ARPU and subscriber retention through a network-based solution for parental controls and content filtering. The integrated solution enables a single policy decision and enforcement point thereby streamlining the number of signaling interactions with external AAA/Policy Manager servers. When used in parallel with other services such as Enhanced Content Charging (ECS) it increases billing accuracy of charging records by insuring that mobile subscribers are only charged for visited sites they are allowed to access.

The Integrated Adult Content Filter is a subscriber-aware inline service provisioned on an ASR 5500 running HA services. Integrated Content Filtering utilizes the local DPI engine and harnesses a distributed software architecture that scales with the number of active HA sessions on the system.

Content Filtering policy enforcement is the process of deciding if a subscriber should be able to receive some content. Typical options are to allow, block, or replace/redirect the content based on the rating of the content and the policy defined for that content and subscriber. The policy definition is transferred in an authentication response from a AAA server or Diameter policy message via the Gx reference interface from an adjunct PCRF. The policy is applied to subscribers through rulebase or APN/Subscriber configuration. The policy determines the action to be taken on the content request on the basis of its category. A maximum of one policy can be associated with a rulebase.

ICAP Interface

Provides a value-added service to prevent unintended viewing of objectionable content that exploits underage children. Content Filtering offers mobile operators a way to increase data ARPU and subscriber retention through a network-based solution for parental controls and content filtering. The Content Filtering ICAP solution is appropriate for operators with existing installations of Active Content Filtering servers in their networks.

The Enhanced Charging Service (ECS) provides a streamlined Internet Content Adaptation Protocol (ICAP) interface to leverage the Deep Packet Inspection (DPI) to enable external Application Servers to provide their services without performing the DPI functionality and without being inserted in the data flow. The ICAP interface may be attractive to mobile operators that prefer to use an external Active Content Filtering (ACF) Platform. If a subscriber initiates a WAP (WAP1.x or WAP2.0) or Web session, the subsequent GET/POST request is detected by the deep packet inspection function. The URL of the GET/POST request is extracted by the local DPI engine on the ASR 5500 platform and passed, along with subscriber identification information and the subscriber request, in an ICAP message to the Application Server (AS). The AS 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 the GET/POST message. Depending upon the response received from the ACF server, the HA either passes the request unmodified or discards the message and responds to the subscriber with the appropriate redirection or block message.

IPNE Service Support

The HA supports the IP Network Enabler (IPNE) service. IPNE is a Mobile and IP Network Enabler (MINE) client component that collects and distributes session and network information to MINE servers. The MINE cloud service provides a central portal forwireless operators and partners to share and exchange session and network information to realize intelligent services. For detailedinformation on IPNE, refer to the *IP Network Enabler* appendix in this guide.

Network Address Translation (NAT)

NAT translates non-routable private IP address(es) to routable public IP address(es) from a pool of public IP addresses that have been designated for NAT. This enables to conserve on the number of public IP addresses required to communicate with external networks, and ensures security as the IP address scheme for the internal network is masked from external hosts, and each outgoing and incoming packet goes through the translation process.

NAT works by inspecting both incoming and outgoing IP datagrams and, as needed, modifying the source IP address and port number in the IP header to reflect the configured NAT address mapping for outgoing datagrams. The reverse NAT translation is applied to incoming datagrams.

NAT can be used to perform address translation for simple IP and mobile IP. NAT can be selectively applied/denied to different flows (5-tuple connections) originating from subscribers based on the flows' L3/L4 characteristicsSource-IP, Source-Port, Destination-IP, Destination-Port, and Protocol.

NAT supports the following mappings:

- One-to-One
- Many-to-One

Important For more information on NAT, refer to the *Network Address Translation Administration Guide.*

Personal Stateful Firewall

The Personal Stateful Firewall is an in-line service feature that inspects subscriber traffic and performs IP session-based access control of individual subscriber sessions to protect the subscribers from malicious security attacks.

The Personal Stateful Firewall supports stateless and stateful inspection and filtering based on the configuration.

In stateless inspection, the firewall inspects a packet to determine the 5-tuplesource and destination IP addresses and ports, and protocolinformation contained in the packet. This static information is then compared against configurable rules to determine whether to allow or drop the packet. In stateless inspection the firewall examines each packet individually, it is unaware of the packets that have passed through before it, and has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is a rogue packet.

In stateful inspection, the firewall not only inspects packets up through the application layer / layer 7 determining a packet's header information and data content, but also monitors and keeps track of the connection's state. For all active connections traversing the firewall, the state information, which may include IP addresses and ports involved, the sequence numbers and acknowledgement numbers of the packets traversing the connection, TCP packet flags, etc. is maintained in a state table. Filtering decisions are based not only on rules but also on the connection state established by prior packets on that connection. This enables to prevent a variety of DoS, DDoS, and other security violations. Once a connection is torn down, or is timed out, its entry in the state table is discarded.

The Enhanced Charging Service (ECS) / Active Charging Service (ACS) in-line service is the primary vehicle that performs packet inspection and charging. For more information on ECS, see the *Enhanced Charging Service Administration Guide*.

Important For more information on Personal Stateful Firewall, refer to the *Personal Stateful Firewall Administration Guide*.

Supported Standards

The system supports the following industry standards for 1x/CDMA2000/EV-DO devices.

Requests for Comments (RFCs)

- RFC-768, User Datagram Protocol (UPD), August 1980
- RFC-791, Internet Protocol (IP), September 1982
- RFC-793, Transmission Control Protocol (TCP), September 1981
- RFC-894, A Standard for the Transmission of IP Datagrams over Ethernet Networks, April 1984
- RFC-1089, SNMP over Ethernet, February 1989
- RFC-1144, Compressing TCP/IP headers for low-speed serial links, February 1990
- RFC-1155, Structure and Identification of Management Information for TCP/IP-based Internets, May 1990
- RFC-1157, Simple Network Management Protocol (SNMP) Version 1, May 1990
- RFC-1212, Concise MIB Definitions, March 1991
- RFC-1213, Management Information Base for Network Management of TCP/IP-based Internets: MIB-II, March 1991
- RFC-1215, A Convention for Defining Traps for use with the SNMP, March 1991
- RFC-1224, Techniques for Managing Asynchronously Generated Alerts, May 1991
- RFC-1256, ICMP Router Discovery Messages, September 1991
- RFC-1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis, March 1992
- RFC-1332, The PPP Internet Protocol Control Protocol (IPCP), May 1992
- RFC-1398, Definitions of Managed Objects for the Ethernet-Like Interface Types, January 1993
- RFC-1418, SNMP over OSI, March 1993
- RFC-1570, PPP LCP Extensions, January 1994
- RFC-1643, Definitions of Managed Objects for the Ethernet-like Interface Types, July 1994
- RFC-1661, The Point to Point Protocol (PPP), July 1994
- RFC-1662, PPP in HDLC-like Framing, July 1994
- RFC-1701, Generic Routing Encapsulation (GRE), October 1994

- RFC-1771, A Border Gateway Protocol 4 (BGP-4)
- RFC-1850, OSPF Version 2 Management Information Base, November 1995
- RFC-1901, Introduction to Community-based SNMPv2, January 1996
- RFC-1902, Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1903, Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1904, Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1905, Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1906, Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1907, Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1908, Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework, January 1996
- RFC-1918, Address Allocation for Private Internets, February 1996
- RFC-1919, Classical versus Transparent IP Proxies, March 1996
- RFC-1962, The PPP Compression Control Protocol (CCP), June 1996
- RFC-1974, PPP STAC LZS Compression Protocol, August 1996
- RFC-2002, IP Mobility Support, May 1995
- RFC-2003, IP Encapsulation within IP, October 1996
- RFC-2004, Minimal Encapsulation within IP, October 1996
- RFC-2005, Applicability Statement for IP Mobility Support, October 1996
- RFC-2118, Microsoft Point-to-Point Compression (MPPC) Protocol, March 1997
- RFC-2136, Dynamic Updates in the Domain Name System (DNS UPDATE)
- RFC-2211, Specification of the Controlled-Load Network Element Service
- RFC-2246, The Transport Layer Security (TLS) Protocol Version 1.0, January 1999
- RFC-2290, Mobile IPv4 Configuration Option for PPP IPCP, February 1998
- RFC-2328, OSPF Version 2, April 1998
- RFC-2344, Reverse Tunneling for Mobile IP, May 1998
- RFC-2394, IP Payload Compression Using DEFLATE, December 1998
- RFC-2401, Security Architecture for the Internet Protocol, November 1998

- RFC-2402, IP Authentication Header (AH), November 1998
- RFC-2406, IP Encapsulating Security Payload (ESP), November 1998
- RFC-2408, Internet Security Association and Key Management Protocol (ISAKMP), November 1998
- RFC-2409, The Internet Key Exchange (IKE), November 1998
- RFC-2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998
- RFC-2475, An Architecture for Differentiated Services, December 1998
- RFC-2484, PPP LCP Internationalization Configuration Option, January 1999
- RFC-2486, The Network Access Identifier (NAI), January 1999
- RFC-2571, An Architecture for Describing SNMP Management Frameworks, April 1999
- RFC-2572, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), April 1999
- RFC-2573, SNMP Applications, April 1999
- RFC-2574, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), April 1999
- RFC-2597, Assured Forwarding PHB Group, June 1999
- RFC2598 - Expedited Forwarding PHB, June 1999
- RFC-2618, RADIUS Authentication Client MIB, June 1999
- RFC-2620, RADIUS Accounting Client MIB, June 1999
- RFC-2661, Layer Two Tunneling Protocol "L2TP", August 1999
- RFC-2697, A Single Rate Three Color Marker, September 1999
- RFC-2698, A Two Rate Three Color Marker, September 1999
- RFC-2784, Generic Routing Encapsulation (GRE) - March 2000, IETF
- RFC-2794, Mobile IP Network Access Identifier Extension for IPv4, March 2000
- RFC-2809, Implementation of L2TP Compulsory Tunneling via RADIUS, April 2000
- RFC-2845, Secret Key Transaction Authentication for DNS (TSIG), May 2000
- RFC-2865, Remote Authentication Dial In User Service (RADIUS), June 2000
- RFC-2866, RADIUS Accounting, June 2000
- RFC-2867, RADIUS Accounting Modifications for Tunnel Protocol Support, June 2000
- RFC-2868, RADIUS Attributes for Tunnel Protocol Support, June 2000
- RFC-2869, RADIUS Extensions, June 2000
- RFC-3007, Secure Domain Name System (DNS) Dynamic Update, November 2000
- RFC-3012, Mobile IPv4 Challenge/Response Extensions, November 2000

- RFC-3095, Robust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP and uncompressed, July 2001
- RFC-3101, OSPF NSSA Option, January 2003.
- RFC-3141, CDMA2000 Wireless Data Requirements for AAA, June 2001
- RFC-3143, Known HTTP Proxy/Caching Problems, June 2001
- RFC-3193, Securing L2TP using IPSEC, November 2001
- RFC-3241 Robust Header Compression (ROHC) over PPP, April 2002
- RFC-3409, Lower Layer Guidelines for Robust (RTP/UDP/IP) Header Compression, December 2002
- RFC-3519, NAT Traversal for Mobile IP, April 2003
- RFC-3543, Registration Revocation in Mobile IPv4, August 2003
- RFC 3576 - Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), July 2003
- RFC-3706, A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers, February 2004
- RFC-3759, Robust Header Compression (ROHC): Terminology and Channel Mapping Examples, April 2004
- RFC-3588, Diameter Based Protocol, September 2003
- RFC-4005, Diameter Network Access Server Application, August 2005
- RFC-4006, Diameter Credit-Control Application, August 2005
- Draft, Generalized Key Distribution Extensions for Mobile IP
- Draft, AAA Keys for Mobile IP

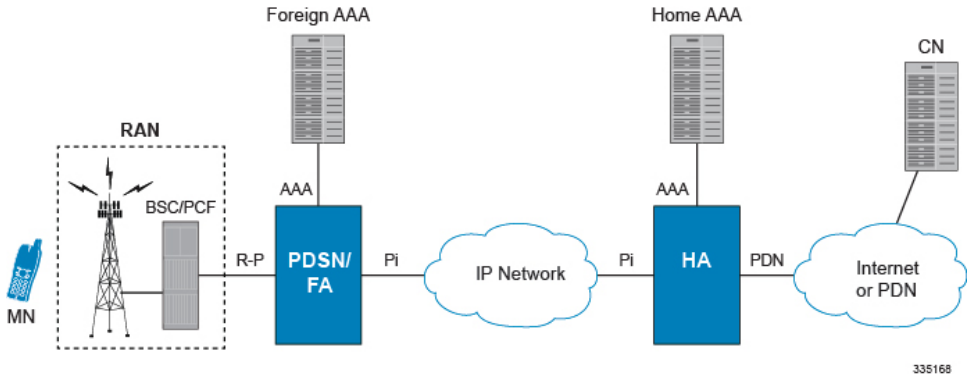
Network Deployment Configurations

This section provides examples of how the system can be deployed within a wireless carrier\'s network. As noted previously in this chapter, the system can be deployed in standalone configurations, serving as a Home Agent (HA) and a Packet Data Serving Node/Foreign Agent (PDSN/FA), or in a combined PDSN/FA/HA configuration providing all services from a single chassis.

Standalone PDSN/FA and HA Deployments

The following figure depicts a sample network configuration wherein the HA and the PDSN/FA are separate systems.

Figure 1: PDSN/FA and HA Network Deployment Configuration Example



The HA allows mobile nodes to be reached, or served, by their home network through its home address even when the mobile node is not attached to its home network. The HA performs this function through interaction with an FA that the mobile node is communicating with using the Mobile IP protocol. Such transactions are performed through the use of virtual private networks that create Mobile IP tunnels between the HA and FA.

Interface Descriptions

This section describes the primary interfaces used in a CDMA2000 wireless data network deployment.

Pi Interfaces

The Pi interface provides connectivity between the HA and its corresponding FA. The Pi interface is used to establish a Mobile IP tunnels between the PDSN/FA and HA.

PDN Interfaces

PDN interface provide connectivity between the PDSN and/or HA to packet data networks such as the Internet or a corporate intranet.

AAA Interfaces

Using the LAN ports located on the Switch Processor I/O (SPIO) and Ethernet line cards, these interfaces carry AAA messages to and from RADIUS accounting and authentication servers. The SPIO supports RADIUS-capable management interfaces using either copper or fiber Ethernet connectivity through two auto-sensing 10/100/1000 Mbps Ethernet interfaces or two SFP optical gigabit Ethernet interfaces. User-based RADIUS messaging is transported using the Ethernet line cards.

While most carriers will configure separate AAA interfaces to allow for out-of-band RADIUS messaging for system administrative users and other operations personnel, it is possible to use a single AAA interface hosted on the Ethernet line cards to support a single RADIUS server that supports both management users and network users.

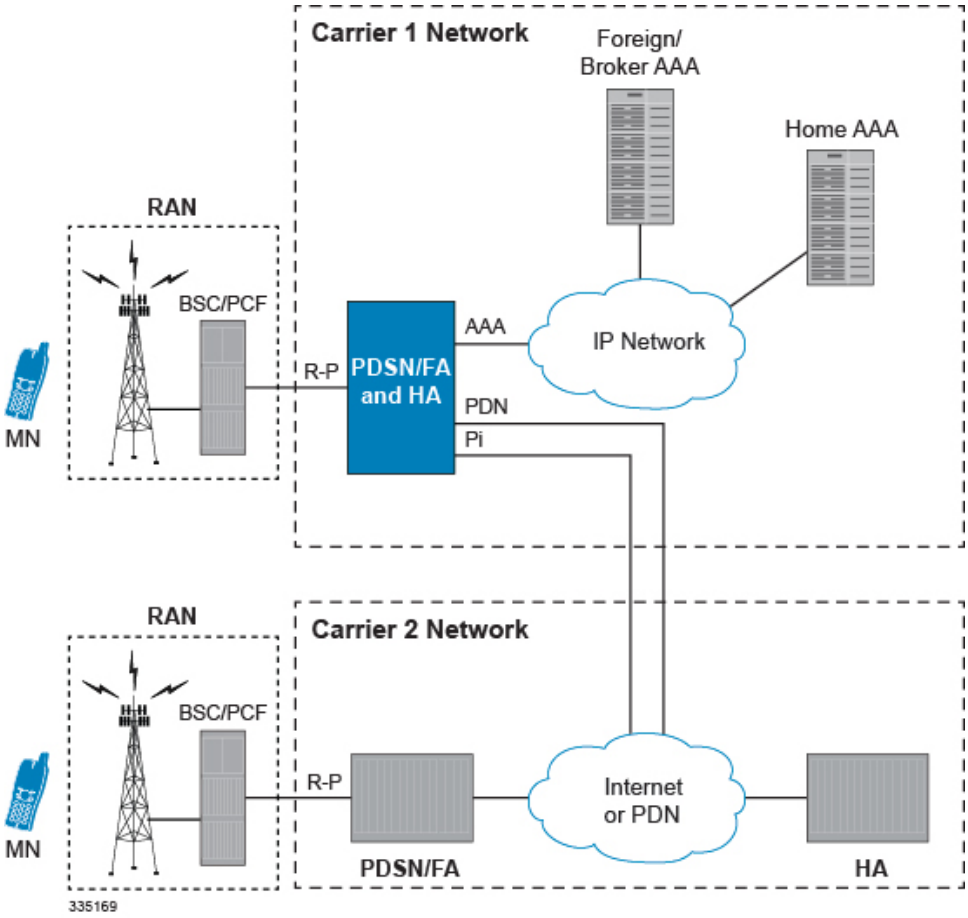
Important Subscriber AAA interfaces should always be configured using Ethernet line card interfaces for the highest performance. The local context should not be used for service subscriber AAA functions.

Co-Located Deployments

An advantage of the system is its ability to support both high-density HA and PDSN/FA configurations within the same chassis. The economies of scale presented in this configuration example provide for both improved session handling and reduced cost in deploying a CDMA2000 data network.

The following figure depicts a sample co-located deployment.

Figure 2: Co-located PDSN/FA and HA Configuration Example



It should be noted that all interfaces defined within the 3GPP2 standards for 1x deployments exist in this configuration as they are described in the two previous sections. This configuration can support communications to external, or standalone, HAs and/or PDSNs/FAs using all prescribed standards.

Mobile IP Tunneling Methods

Tunneling by itself is a technology that enables one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within a packet, carried by the second network. Tunneling is also called encapsulation. Service providers typically use tunneling for two purposes; first, to transport otherwise un-routable packets across the IP network and second, to provide data separation for Virtual Private Networking (VPN) services. In Mobile IP, tunnels are used to transport data packets between the FA and HA.

The system supports the following tunneling protocols, as defined in the IS-835-A specification and the relevant Request For Comments (RFCs) for Mobile IP:

IP in IP tunnels

IP in IP tunnels basically encapsulate one IP packet within another using a simple encapsulation technique. To encapsulate an IP datagram using IP in IP encapsulation, an outer IP header is inserted before the datagram's existing IP header. Between them are other headers for the path, such as security headers specific to the tunnel configuration. Each header chains to the next using IP Protocol values. The outer IP header Source and Destination identify the "endpoints" of the tunnel. The inner IP header Source and Destination identify the original sender and recipient of the datagram, while the inner IP header is not changed by the encapsulator, except to decrement the TTL, and remains unchanged during its delivery to the tunnel exit point. No change to IP options in the inner header occurs during delivery of the encapsulated datagram through the tunnel. If needed, other protocol headers such as the IP Authentication header may be inserted between the outer IP header and the inner IP header.

The Mobile IP working group has specified the use of encapsulation as a way to deliver datagrams from an MN's HA to an FA, and conversely from an FA to an HA, that can deliver the data locally to the MN at its current location.

GRE tunnels

The Generic Routing Encapsulation (GRE) protocol performs encapsulation of IP packets for transport across disparate networks. One advantage of GRE over earlier tunneling protocols is that any transport protocol can be encapsulated in GRE. GRE is a simple, low overhead approachthe GRE protocol itself can be expressed in as few as eight octets as there is no authentication or tunnel configuration parameter negotiation. GRE is also known as IP Protocol 47.

Important The chassis simultaneously supports GRE protocols with key in accordance with RFC-1701/RFC-2784 and "Legacy" GRE protocols without key in accordance to RFC-2002.

Another advantage of GRE tunneling over IP-in-IP tunneling is that GRE tunneling can be used even when conflicting addresses are in use across multiple contexts (for the tunneled data).

Communications between the FA and HA can be done in either the forward or reverse direction using the above protocols. Additionally, another method of routing information between the FA and various content servers used by the HA exists. This method is called Triangular Routing. Each of these methods is explained below.

Forward Tunneling

In the wireless IP world, forward tunneling is a tunnel that transports packets from the packet data network towards the MN. It starts at the HA and ends at the MN's care-of address. Tunnels can be as simple as IP-in-IP tunnels, GRE tunnels, or even IP Security (IPSec) tunnels with encryption. These tunnels can be started automatically, and are selected based on the subscriber's user profile.

Reverse Tunneling

A reverse tunnel starts at the MN's care-of address, which is the FA, and terminates at the HA.

When an MN arrives at a foreign network, it listens for agent advertisements and selects an FA that supports reverse tunnels. The MN requests this service when it registers through the selected FA. At this time, the MN may also specify a delivery technique such as Direct or the Encapsulating Delivery Style.

Using the Direct Delivery Style, which is the default mode for the system, the MN designates the FA as its default router and sends packets directly to the FA without encapsulation. The FA intercepts them, and tunnels them to the HA.

Using the Encapsulating Delivery Style, the MN encapsulates all its outgoing packets to the FA. The FA then de-encapsulates and re-tunnels them to the HA, using the FA's care-of address as the entry-point for this new tunnel.

Following are some of the advantages of reverse tunneling:

- All datagrams from the mobile node seem to originate from its home network
- The FA can keep track of the HA that the mobile node is registered to and tunnel all datagrams from the mobile node to its HA

Triangular Routing

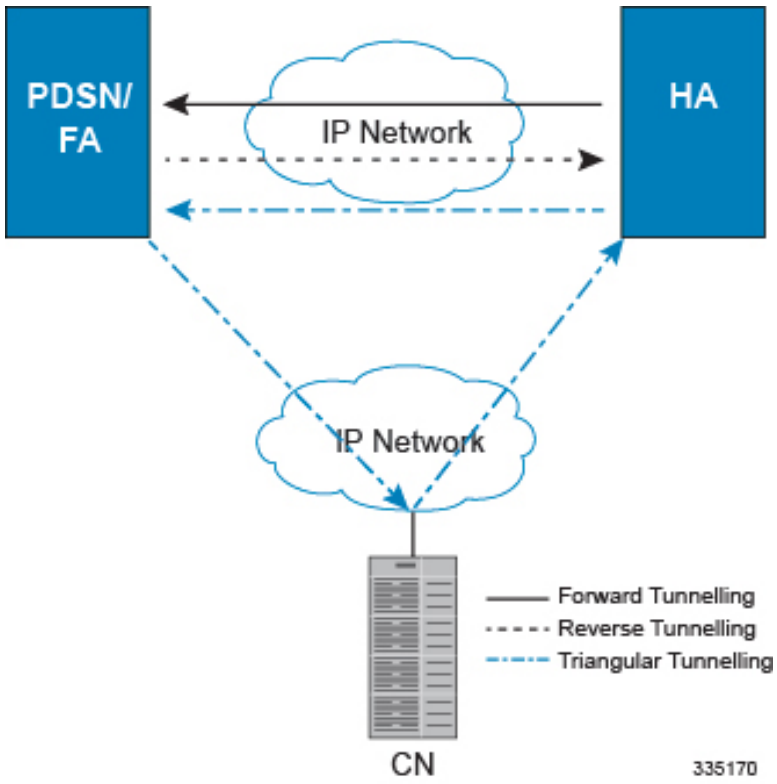
Triangular routing is the path followed by a packet from the MN to the Correspondent Node (CN) via the FA. In this routing scenario, the HA receives all the packets destined to the MN from the CN and redirects them to the MN's care-of-address by forward tunneling. In this case, the MN sends packets to the FA, which are transported using conventional IP routing methods.

A key advantage of triangular routing is that reverse tunneling is not required, eliminating the need to encapsulate and de-capsulate packets a second time during a Mobile IP session since only a forward tunnel exists between the HA and PDSN/FA.

A disadvantage of using triangular routing is that the HA is unaware of all user traffic for billing purposes. Also, both the HA and FA are required to be connected to a private network. This can be especially troublesome in large networks, serving numerous enterprise customers, as each FA would have to be connected to each private network.

The following figure shows an example of how triangular routing is performed.

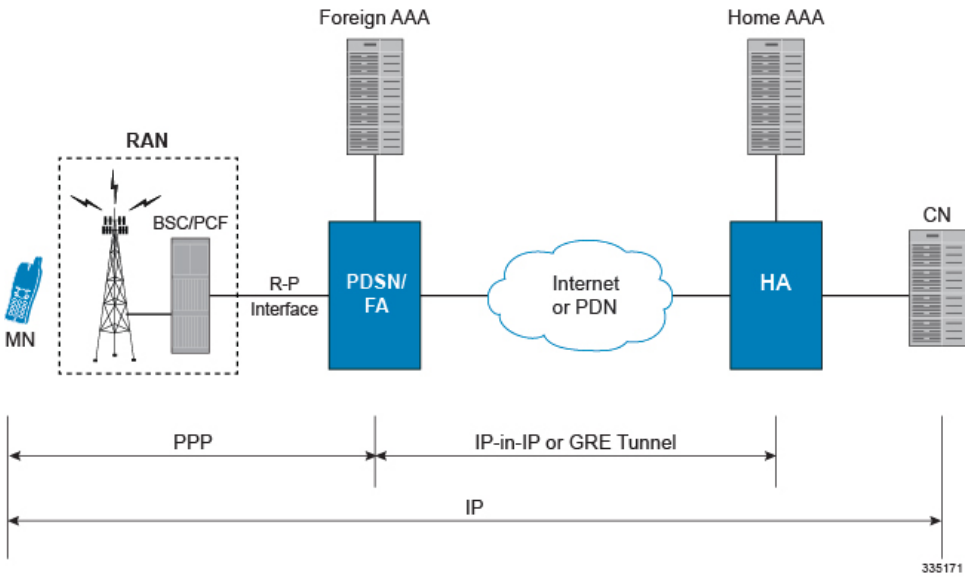
Figure 3: Mobile IP, FA and HA Tunneling/Transport Methods



How Mobile IP Works

As described earlier, Mobile IP uses three basic communications protocols; PPP, IP, and Tunneled IP in the form of IP-in-IP or GRE tunnels. The following figure depicts where each of these protocols are used in a basic Mobile IP call.

Figure 4: Mobile IP Protocol Usage



As depicted above, PPP is used to establish a communications session between the MN and the FA. Once a PPP session is established, the MN can communicate with the HA, using the FA as a mediator or broker. Data transport between the FA and HA use tunneled IP, either IP-in-IP or GRE tunneling. Communication between the HA and End Host can be achieved using the Internet or a private IP network and can use any IP protocol.

The following figure provides a high-level view of the steps required to make a Mobile IP call that is initiated by the MN to a HA. The following table explains each step in detail. Users should keep in mind that steps in the call flow related to the Radio Access Node (RAN) functions are intended to show a high-level overview of radio communications iterations, and as such are outside the scope of packet-based communications presented here.

Figure 5: Mobile IP Call Flow

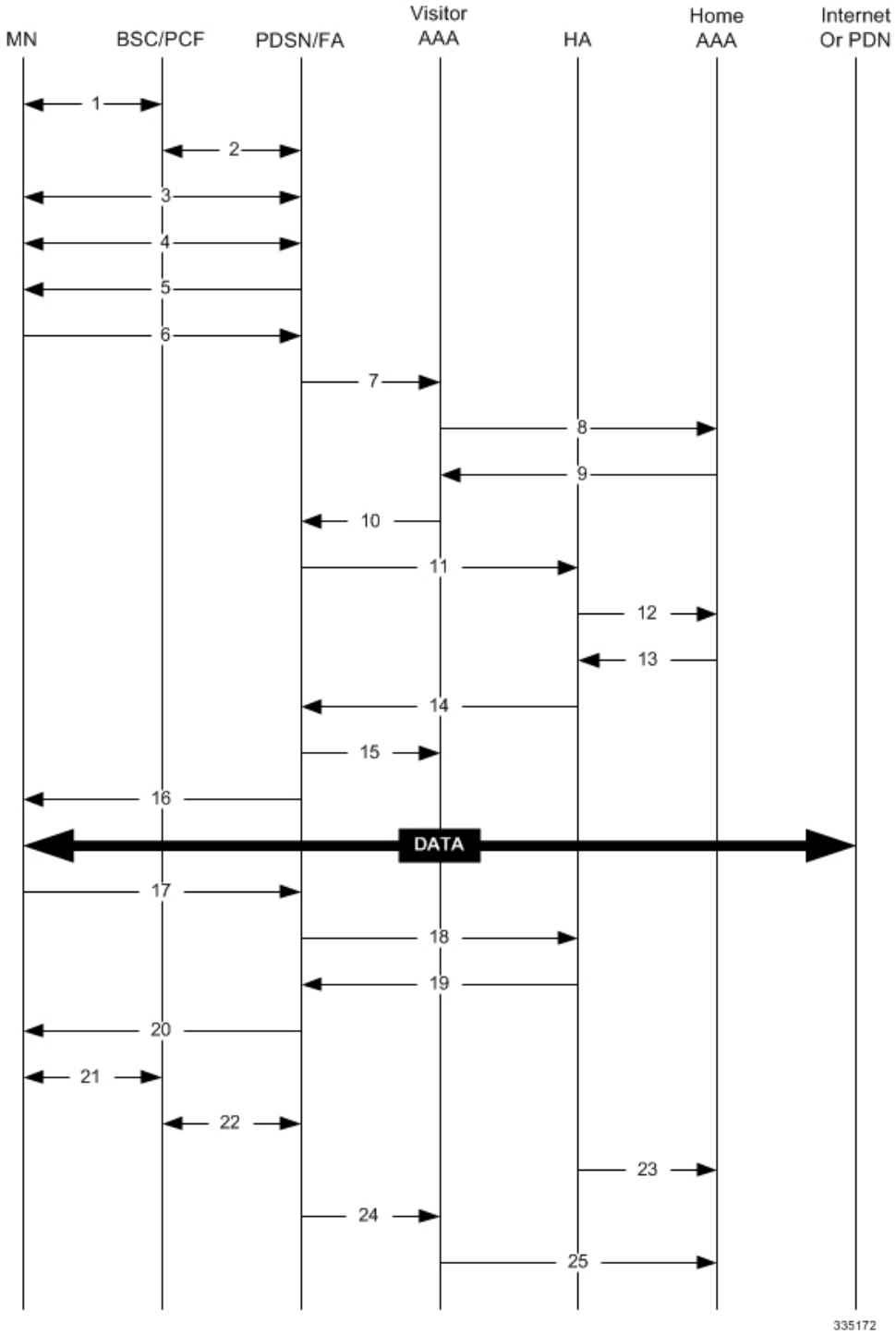


Table 1: Mobile IP Call Flow Description

Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the RAN through the BSC/PCF.
2	The PCF and PDSN establish the R-P interface for the session.
3	The PDSN and MN negotiate Link Control Protocol (LCP).
4	The PDSN and MN negotiate the Internet Protocol Control Protocol (IPCP).
5	The PDSN/FA sends an Agent Advertisement to the MN.
6	The MN sends a Mobile IP Registration Request to the PDSN/FA.
7	The PDSN/FA sends an Access Request message to the visitor AAA server.
8	The visitor AAA server proxies the request to the appropriate home AAA server.
9	The home AAA server sends an Access Accept message to the visitor AAA server.
10	The visitor AAA server forwards the response to the PDSN/FA.
11	Upon receipt of the response, the PDSN/FA forwards a Mobile IP Registration Request to the appropriate HA.
12	The HA sends an Access Request message to the home AAA server to authenticate the MN/subscriber.
13	The home AAA server returns an Access Accept message to the HA.
14	Upon receiving response from home AAA, the HA sends a reply to the PDSN/FA establishing a forward tunnel. Note that the reply includes a Home Address (an IP address) for the MN.
15	The PDSN/FA sends an Accounting Start message to the visitor AAA server. The visitor AAA server proxies messages to the home AAA server as needed.
16	The PDSN return a Mobile IP Registration Reply to the MN establishing the session allowing the MN to send/receive data to/from the PDN.

Step	Description
17	Upon session completion, the MN sends a Registration Request message to the PDSN/FA with a requested lifetime of 0.
18	The PDSN/FA forwards the request to the HA.
19	The HA sends a Registration Reply to the PDSN/FA accepting the request.
20	The PDSN/FA forwards the response to the MN.
21	The MN and PDSN/FA negotiate the termination of LCP effectively ending the PPP session.
22	The PCF and PDSN/FA close terminate the R-P session.
23	The HA sends an Accounting Stop message to the home AAA server.
24	The PDSN/FA sends an Accounting Stop message to the visitor AAA server.
25	The visitor AAA server proxies the accounting data to the home AAA server.

Understanding Mobile IP

Mobile IP provides a network-layer solution that allows Mobile Nodes (MNs, i.e. mobile phones, wireless PDAs, and other mobile devices) to receive routed IP packets from their home network while they are connected to any visitor network using their permanent or home IP address. Mobile IP allows mobility in a dynamic method that allows nodes to maintain ongoing communications while changing links as the user traverses the global Internet from various locations outside their home network.

In Mobile IP, the Mobile Node (MN) receives an IP address, either static or dynamic, called the "home address" assigned by its Home Agent (HA). A distinct advantage with Mobile IP is that MNs can hand off between different radio networks that are served by different PDSNs.

In this scenario, the Network Access Function (such as a PDSN) in the visitor network performs as a Foreign Agent (FA), establishing a virtual session with the MN's HA. Each time the MN registers with a different PDSN/FA, the FA assigns the MN a care-of-address. Packets are then encapsulated into IP tunnels and transported between FA, HA, and the MN.

Session Continuity Support for 3GPP2 and WiMAX Handoffs

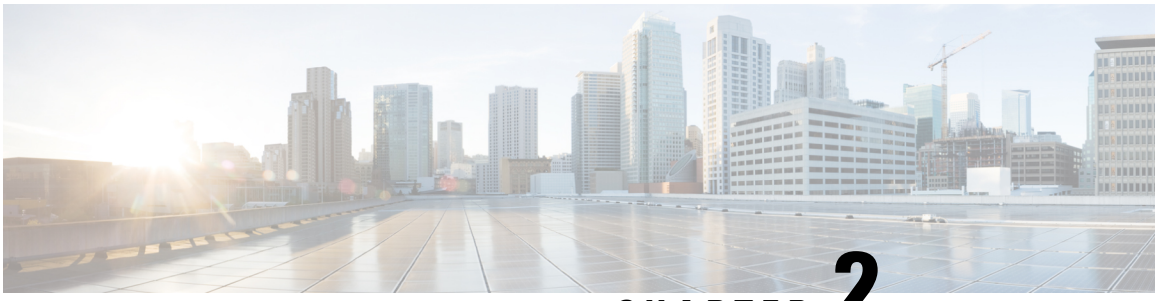
HA provides this feature for seamless session mobility for WiMAX subscriber and other access technology subscribers as well. By implementation of this feature HA can be configured for:

- 3GPP2 HA Service
- 3GPP HA Service
- WiMAX HA Service

- Combination of 3GPP2 and WiMAX HA Services for Dual mode device

The above configurations provide the session continuity capability that enables a dual mode device (a multi radio device) to continue its active data session as it changes its active network attachment from 3GPP2 to Wimax and vice versa with no perceived user impacts from a user experience perspective. This capability brings the following benefits:

- common billing and customer care
- accessing home 3GPP2 service through Wimax network and vice versa
- better user experience with seamless session continuity



CHAPTER 2

Mobile IP Configuration Examples

This chapter provides information for several configuration examples that can be implemented on the system to support Mobile IP (MIP) data services.

Important This chapter does not discuss the configuration of the local context. Information about the local context can be found in Chapter 1 of Command Line Reference. Additionally, when configuring Mobile IP take into account the MIP timing considerations discussed in *Mobile-IP and Proxy-MIP Timer Considerations*.

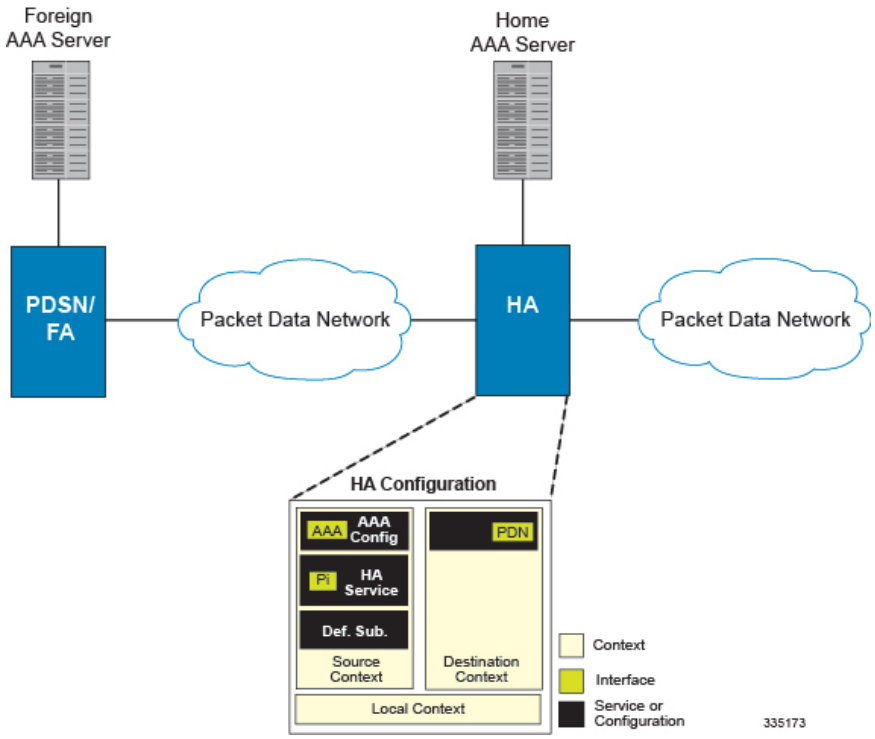
This chapter includes the following examples:

Example 1: Mobile IP Support Using the System as an HA

The system supports both Simple and Mobile IP. For Mobile IP applications, the system can be configured to perform the function of a PDSN/FA and/or a HA. This example describes what is needed for and how the system performs the role of the HA. Example number 1 provides information on using the system to provide PDSN/FA functionality.

The system\'s HA configuration for Mobile IP applications requires that at least two contexts (one source and one destination) be configured as shown in the following figure.

Figure 6: Mobile IP Support Using the system as an HA



The source context will facilitate the HA service(s), the Pi interfaces from the FA, and the AAA interfaces. The source context will also be configured to provide Home AAA functionality for subscriber sessions. The destination context will facilitate the PDN interface(s).

Information Required

Prior to configuring the system as shown in this example, there is a minimum amount of information required. The following sections describe the information required to configure the source and destination contexts.

Source Context Configuration

The following table lists the information that is required to configure the source context.

Table 2: Required Information for Source Context Configuration

Required Information	Description
Source context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the source context will be recognized by the system. **Important** The name of the source context should be the same as the name of the context in which the FA-context is configured if a separate system is being used to provide PDSN/FA functionality.

Required Information	Description
Pi Interface Configuration	
Pi interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. Pi interfaces are configured in the destination context. If this interface is being used for Interchassis Session Recovery, you must specify a loopback interface type after the interface_name.
IP address and subnet	These will be assigned to the Pi interfaces.Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical Pi interfaces.
Gateway IP address(es)	Used when configuring static routes from the Pi interfaces to a specific network.
HA service Configuration	
HA service name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the HA service will be recognized by the system. Multiple names are needed if multiple HA services will be used. HA services are configured in the destination context.

Required Information	Description
UDP port number for Mobile IP traffic	Specifies the port used by the HA service and the FA for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 434.
Mobile node re-registration requirements	Specifies how the system should handle authentication for mobile node re-registrations.The HA service can be configured as follows: • Always require authentication • Never require authentication. **Important** (the initial registration and de-registration will still be handled normally) • Never look for mn-aaa extension • Not require authentication but will authenticate if mn-aaa extension present

Required Information	Description
FA-to-HA Security Parameter Index Information	**FA IP address:** The HA service allows the creation of a security profile that can be associated with a particular FA. This specifies the IP address of the FA that the HA service will be communicating with. Multiple FA addresses are needed if the HA will be communicating with multiple FAs.
	Index: Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.
	Secret: Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is hmac-md5.A hash-algorithm is required for each SPI configured.

Required Information	Description
Mobile Node Security Parameter Index Information	**Index:** Specifies the shared SPI between the HA service and the mobile node(s). The SPI can be configured to any integer value between 256 and 4294967295.Multiple SPIs can be configured if the HA service is to communicate with multiple mobile nodes.
	Secret(s): Specifies the shared SPI secret between the HA service and the mobile node. The secret can be between 1 and 127 characters (alpha and/or numeric).An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is hmac-md5.A hash-algorithm is required for each SPI configured.
	Replay-protection process: Specifies how protection against replay-attacks is implemented. The possible processes are nonce and timestamp. The default is timestamp with a tolerance of 60 seconds. A replay-protection process is required for each mobile node-to-HA SPI configured.
Maximum registration lifetime	Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node. The time is measured in seconds and can be configured to any integer value between 1 and 65534. An infinite registration lifetime can also be configured by disabling the timer. The default is 600.

Required Information	Description
Maximum number of simultaneous bindings	Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address. The number can be configured to any integer value between 1 and 5. The default is 3.
AAA Interface Configuration	
AAA interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. AAA interfaces will be configured in the source context.
IP address and subnet	These will be assigned to the AAA interface.Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
Home RADIUS Server Configuration	

Required Information	Description
Home RADIUS Authentication server	IP Address: Specifies the IP address of the home RADIUS authentication server the source context will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers will be configured.Home RADIUS authentication servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the home RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.

Required Information	Description
Home RADIUS Accounting server	IP Address: Specifies the IP address of the home RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured. Home RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS accounting server and the source context.A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the home RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the home RADIUS server. The name must be between 1 and 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the source context\'s AAA interface. A secondary address can be optionally configured.
Default Subscriber Configuration	
"Default" subscriber\'s IP context name	Specifies the name of the egress context on the system that facilitates the PDN ports. **Important** For this configuration, the IP context name should be identical to the name of the destination context.

Destination Context Configuration

Table 3: Required Information for Destination Context Configuration

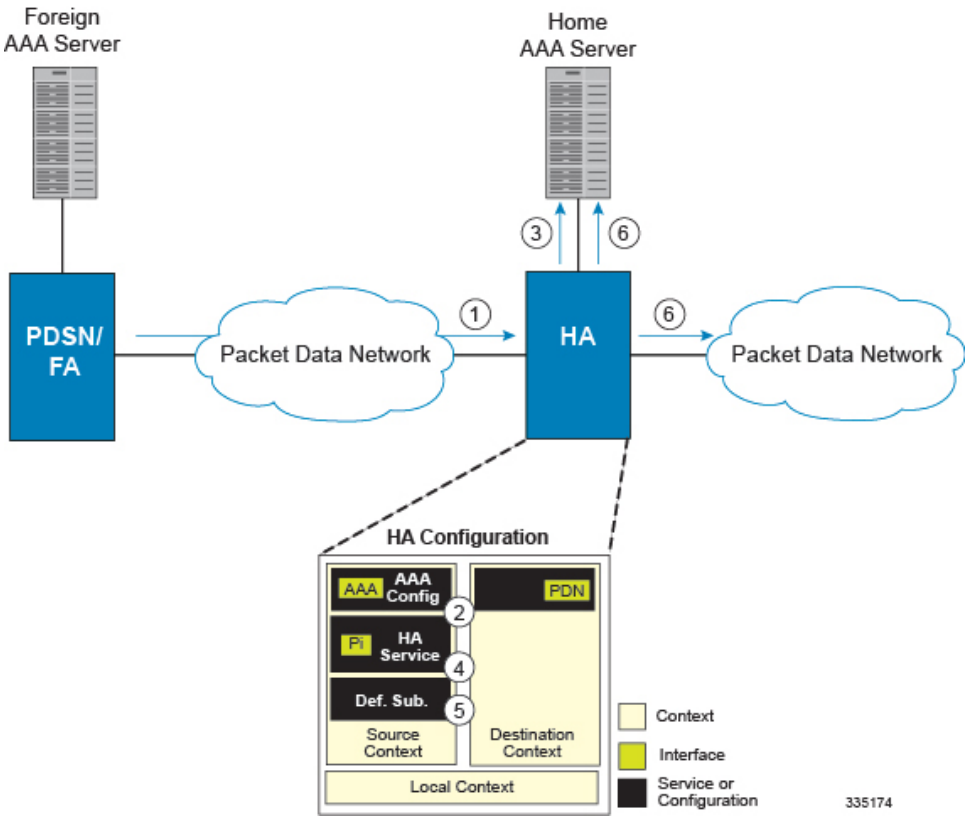
Required Information	Description
Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system. **Important** For this configuration, the destination context name should **not** match the domain name of a specific domain.
PDN Interface Configuration	
PDN interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. PDN interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the PDN interface.Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical PDN interfaces.
Gateway IP address(es)	Used when configuring static routes from the PDN interface(s) to a specific network.
IP Address Pool Configuration	

Required Information	Description
IP address pool name	Each IP address pool is identified by a name. The pool name can be between 1 and 31 alpha and/or numeric characters and is case sensitive. IP address pools are configured in the destination context(s). Multiple address pools can be configured within a single context.
IP pool addresses	An initial address and a subnet, or a starting address and an ending address, are required for each configured pool. The pool will then consist of every possible address within the subnet , or all addresses from the starting address to the ending address.The pool can be configured as public, private, or static. If this IP pool is being used for Interchassis Session Recovery, it must be a static and srp-activated.

How This Configuration Works

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a Mobile IP data call.

Figure 7: Call Processing When Using the system as an HA



1. A subscriber session from the FA is received by the HA service over the Pi interface.
2. The HA service determines which context to use to provide AAA functionality for the session. This process is described in the How the System Selects Contexts section located in the Understanding the System Operation and Configuration chapter of the System Administration Guide.

   For this example, the result of this process is that the HA service determined that AAA functionality should be provided by the Source context.
3. The system then communicates with the Home AAA server specified in the Source context\'s AAA configuration to authenticate the subscriber.
4. Upon successful authentication, the Source context determines which egress context to use for the subscriber session. This process is described in the How the System Selects Contexts section located in the Understanding the System Operation and Configuration chapter of the System Administration Guide.

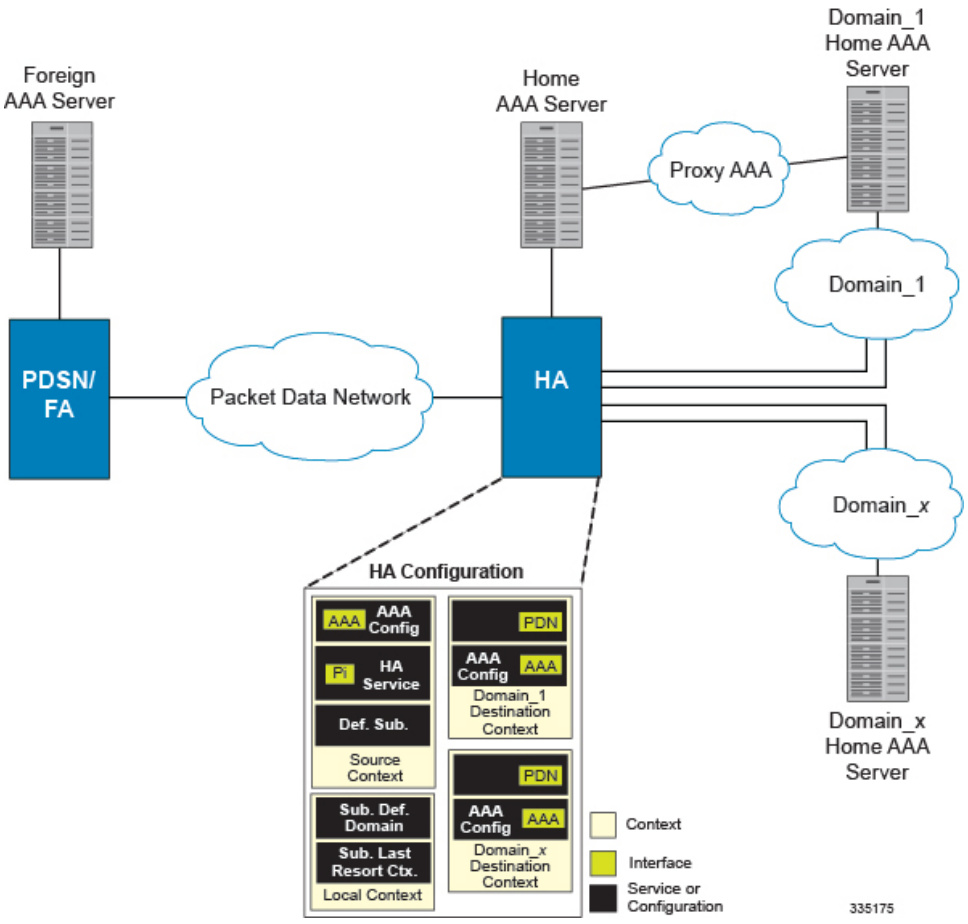
   For this example, the system determines that the egress context is the Destination context based on the configuration of the Default subscriber.
5. An IP address is assigned to the subscriber\'s mobile node from an IP address pool configured in the destination context. This IP address is used for the duration of the session and then be returned to the pool.
6. Data traffic for the subscriber session is then routed through the PDN interface in the Destination context.
7. Accounting messages for the session are sent to the AAA server over the AAA interface.

Example 2: HA Using a Single Source Context and Multiple Outsourced Destination Contexts

The system allows the wireless carrier to easily generate additional revenue by providing the ability to configure separate contexts that can then be leased or outsourced to various enterprises or ISPs, each having a specific domain.

In order to perform the role of an HA and support multiple outsourced domains, the system must be configured with at least one source context and multiple destination contexts as shown in the following figure. The AAA servers could by owned/maintained by either the carrier or the domain. If they are owned by the domain, the carrier will have to receive the AAA information via proxy.

Figure 8: The system as an HA Using a Single Source Context and Multiple Outsourced Destination Contexts



The source context will facilitate the HA service(s), and the Pi interface(s) to the FA(s).The source context will also be configured with AAA interface(s) and to provide Home AAA functionality for subscriber sessions. The destination contexts will each be configured to facilitate PDN interfaces. In addition, because each of the destination contexts can be outsourced to different domains, they will also be configured with AAA interface(s) and to provide AAA functionality for that domain.

In addition to the source and destination contexts, there are additional system-level AAA parameters that must be configured.

Information Required

Prior to configuring the system as shown in this example, there is a minimum amount of information required. The following sections describe the information required to configure the source and destination contexts.

Source Context Configuration

The following table lists the information that is required to configure the source context.

Table 4: Required Information for Source Context Configuration

Required Information	Description
Source context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the source context will be recognized by the system.
Pi Interface Configuration	
Pi interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. Pi interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the Pi interfaces. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical Pi interfaces.

Required Information	Description
Gateway IP address(es)	Used when configuring static routes from the Pi interfaces to a specific network.
HA service Configuration	
HA service name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the HA service will be recognized by the system. Multiple names are needed if multiple HA services will be used. HA services are configured in the destination context.
UDP port number for Mobile IP traffic	Specifies the port used by the HA service and the FA for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 434.
Mobile node re-registration requirements	Specifies how the system should handle authentication for mobile node re-registrations. The HA service can be configured as follows: Always require authentication Never require authentication (**NOTE:** the initial registration and de-registration will still be handled normally) Never look for mn-aaa extension Not require authentication but will authenticate if mn-aaa extension present

Required Information	Description
FA-to-HA Security Parameter Index Information	**FA IP address:** The HA service allows the creation of a security profile that can be associated with a particular FA. This specifies the IP address of the FA that the HA service will be communicating with. Multiple FA addresses are needed if the HA will be communicating with multiple FAs.
	Index: Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.
	Secret: Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is hmac-md5. A hash-algorithm is required for each SPI configured.

Required Information	Description
Mobile Node Security Parameter Index Information	**Index:** Specifies the shared SPI between the HA service and the mobile node(s). The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple mobile nodes.
	Secret(s): Specifies the shared SPI secret between the HA service and the mobile node. The secret can be between 1 and 127 characters (alpha and/or numeric).An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is hmac-md5.A hash-algorithm is required for each SPI configured.
	Replay-protection process: Specifies how protection against replay-attacks is implemented. The possible processes are nonce and timestamp. The default is timestamp with a tolerance of 60 seconds. A replay-protection process is required for each mobile node-to-HA SPI configured.
Maximum registration lifetime	Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node. The time is measured in seconds and can be configured to any integer value between 1 and 65534. An infinite registration lifetime can also be configured by disabling the timer. The default is 600.
Maximum number of simultaneous bindings	Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address. The number can be configured to any integer value between 1 and 5. The default is 3.
AAA Interface Configuration	

Required Information	Description
AAA interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. AAA interfaces will be configured in the source context.
IP address and subnet	These will be assigned to the AAA interface.Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
Home RADIUS Server Configuration	

Required Information	Description
Home RADIUS Authentication server	IP Address: Specifies the IP address of the home RADIUS authentication server the source context will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers will be configured. Home RADIUS authentication servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the home RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.

Required Information	Description
Home RADIUS Accounting server	IP Address:Specifies the IP address of the home RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured. Home RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the home RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the home RADIUS server. The name must be between 1 and 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the source context\'s AAA interface. A secondary address can be optionally configured.
Default Subscriber Configuration	
"Default" subscriber\'s IP context name	Specifies the name of the egress context on the system that facilitates the PDN ports. **Important** For this configuration, the IP context name should be identical to the name of the destination context.

Destination Context Configuration

The following table lists the information required to configure the destination context.

Table 5: Required Information for Destination Context Configuration

Required Information	Description
Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system. **Important** For this configuration, the destination context name should **not** match the domain name of a specific domain.
PDN Interface Configuration	
PDN interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. PDN interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the PDN interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used.Physical ports are configured within the destination context and are used to bind logical PDN interfaces.
Gateway IP address(es)	Used when configuring static routes from the PDN interface(s) to a specific network.
IP Address Pool Configuration	

Required Information	Description
IP address pool name	Each IP address pool is identified by a name. The pool name can be between 1 and 31 alpha and/or numeric characters and is case sensitive. IP address pools are configured in the destination context(s). Multiple address pools can be configured within a single context.
IP pool addresses	An initial address and a subnet, or a starting address and an ending address, are required for each configured pool. The pool will then consist of every possible address within the subnet , or all addresses from the starting address to the ending address. The pool can be configured as public, private, or static. If this IP pool is being used for Interchassis Session Recovery, it must be a static and srp-activated.
AAA Interface Configuration	
AAA interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. AAA interfaces will be configured in the source context.
IP address and subnet	These will be assigned to the AAA interface.Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.

Required Information	Description
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
RADIUS Server Configuration	
RADIUS Authentication server	IP Address: Specifies the IP address of the RADIUS authentication server the source context will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers will be configured. Home RADIUS authentication servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the home RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.

Required Information	Description
RADIUS Accounting server	IP Address:Specifies the IP address of the RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured. Home RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the home RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the home RADIUS server. The name must be between 1 and 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the source context\'s AAA interface. A secondary address can be optionally configured.

System-Level AAA Configuration

The following table lists the information that is required to configure the system-level AAA parameters.

Table 6: Required Information for System-Level AAA Configuration

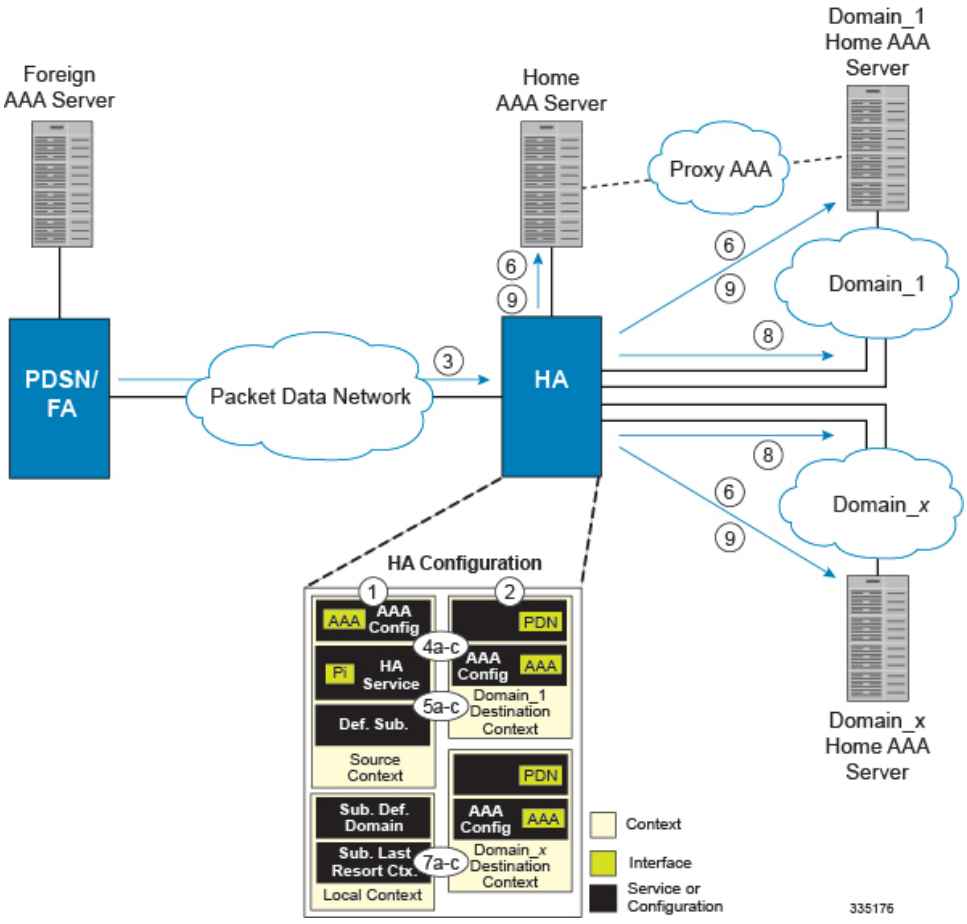
Required Information	Description
Subscriber default domain name	Specifies the name of a context that can provide AAA functions in the event that the domain-part of the username is missing or poorly formed. This parameter will be applied to all subscribers if their domain can not be determined from their username regardless of what domain they are trying to access. **Important** The default domain name can be the same as the source context.
Subscriber Last-resort context	Specifies the name of a context that can provide AAA functions in the event that the domain-part of the username was present but does not match the name of a configured destination context. This parameter will be applied to all subscribers if their specified domain does not match a configured destination context regardless of what domain they are trying to access. **Important** The last-resort context name can be the same as the source context.

Required Information	Description
Subscriber username format	Specifies the format of subscriber usernames as to whether or not the username or domain is specified first and the character that separates them. The possible separator characters are: • @ • % • - • \ • # • / Up to six username formats can be specified. The default is username . **Important** The username string is searched from right to left for the separator character. Therefore, if there is one or more separator characters in the string , only the first one that is recognized is considered the actual separator. For example, if the default username format was used, then for the username string user1@enterprise@isp1, the system resolves to the username user1@enterprise with domain isp1.

How This Configuration Works

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a Mobile IP data call.

Figure 9: Call Processing When Using the system as an HA with a Single Source Context and Multiple Outsourced Destination Contexts

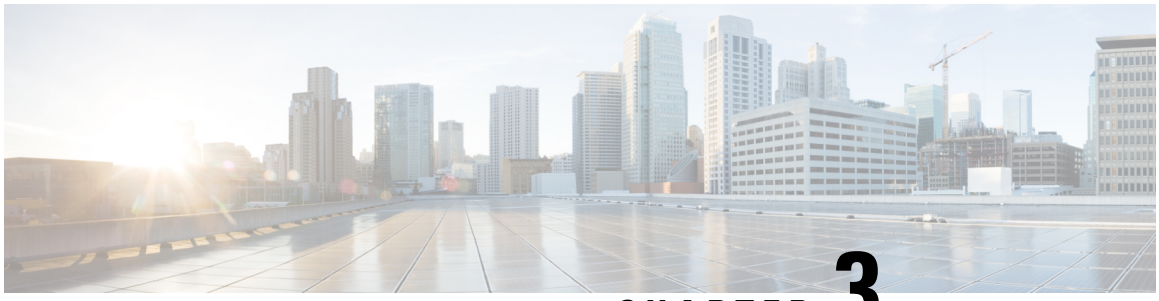


1. A subscriber session from the FA is received by the HA service over the Pi interface.
2. The HA service determines which context to use to provide AAA functionality for the session. This process is described in the How the System Selects Contexts section located in the Understanding the System Operation and Configuration chapter of the System Administration Guide.

   For this example, the result of this process is that the HA service determined that AAA functionality should be provided by the Source context.
3. The system then communicates with the Home AAA server specified in the Source context\'s AAA configuration to authenticate the subscriber.
4. Upon successful authentication, the Source context determines which egress context to use for the subscriber session. This process is described in the How the System Selects Contexts section located in the Understanding the System Operation and Configuration chapter of the System Administration Guide.

   For this example, the system determines that the egress context is the Destination context based on the configuration of the Default subscriber.
5. An IP address is assigned to the subscriber\'s mobile node from an IP address pool configured in the destination context. This IP address is used for the duration of the session and then be returned to the pool.
6. Data traffic for the subscriber session is then routed through the PDN interface in the Destination context.

7. Accounting messages for the session are sent to the AAA server over the AAA interface.



CHAPTER 3

Simple IP and Mobile IP in a Single System Configuration Example

This chapter provides information for several configuration examples that can be implemented on the system to support Simple IP and Mobile IP data services in a single system.

Important This chapter does not discuss the configuration of the localout-of-band management context. Information about the localout-of-band management context can be found in Chapter 1 of *Command Line Reference*. Additionally, when configuring Mobile IP take into account the MIP timing considerations discussed in the section MIP Timer Considerations.

The following topics are covered:

Using the System as Both a PDSN/FA and an HA

The system supports both Simple and Mobile IP. For Mobile IP applications, the system can be configured to perform the function of a Packet Data Service Node/Foreign Agent (PDSN/FA) and/or a Home Agent (HA). This example describes what is needed and how a single system simultaneously supports both of these functions.

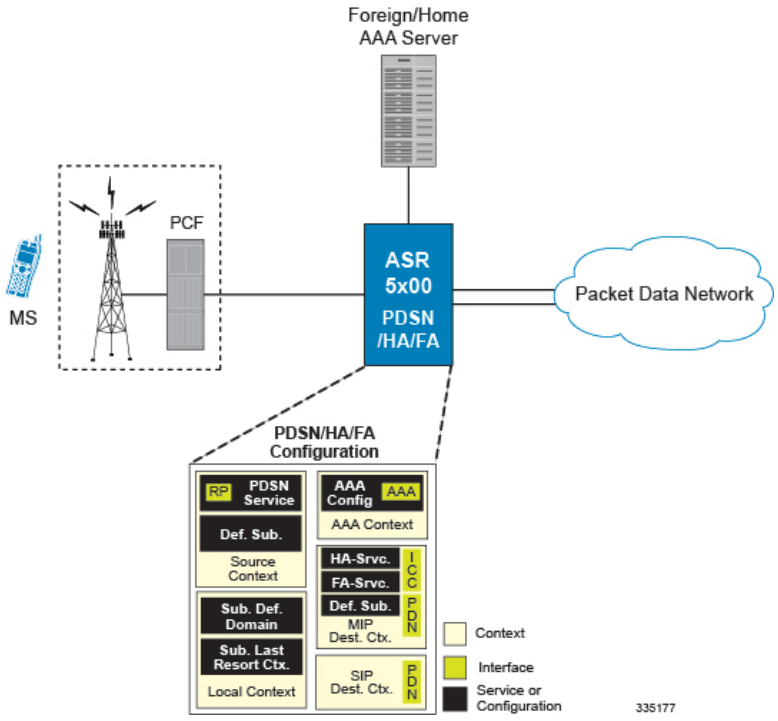
In order to support PDSN, FA, and HA functionality, the system must be configured with at least one source context and at least two destination contexts as shown in the following figure.

The source context will facilitate the PDSN service(s), and the R-P interfaces. The AAA context will be configured to provide foreign/home AAA functionality for subscriber sessions and facilitate the AAA interfaces.

The Mobile IP destination context will be configured to facilitate the FA service, the HA service and the PDN interfaces for Mobile IP data services. The Simple IP destination context will facilitate the PDN interfaces for Simple IP data Services.

In addition to the source and destination contexts, there are additional system-level AAA parameters that must be configured.

Figure 10: Simple and Mobile IP Support Within a Single System



Information Required

Prior to configuring the system as shown in this example, there is a minimum amount of information required. The following sections describe the required information to configure the source and destination contexts.

Source Context Configuration

The following table lists the information that is required to configure the source context.

Table 7: Required Information for Source Context Configuration

Required Information	Description
Source context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the source context will be recognized by the system.
R-P Interface Configuration	
R-P interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. R-P interfaces are configured in the source context.

Required Information	Description
IP address and subnet	These will be assigned to the R-P interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical R-P interfaces.
Gateway IP address	Used when configuring static routes from the R-P interface(s) to a specific network.
PDSN service Configuration	
PDSN service name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the PDSN service will be recognized by the system. Multiple names are needed if multiple PDSN services will be used. PDSN services are configured in the source context.
UDP port number for R-P traffic	Specifies the port used by the PDSN service and the PCF for communications. The UDP port number and can be any integer value between 1 and 65535. The default value is 699.
Authentication protocols used	Specifies how the system handles authentication: using a protocol (such as CHAP, PAP, or MSCHAP), or not requiring any authentication.
Domain alias for NAI-construction	Specifies a context name for the system to use to provide accounting functionality for a subscriber session. This parameter is needed only if the system is configured to support no authentication.

Required Information	Description
Security Parameter Index Information	**PCF IP address:** Specifies the IP address of the PCF that the PDSN service will be communicating with. The PDSN service allows the creation of a security profile that can be associated with a particular PCF. Multiple IP addresses are needed if the PDSN service will be communicating with multiple PCFs.
	Index: Specifies the shared SPI between the PDSN service and a particular PCF. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the PDSN service is to communicate with multiple PCFs.
	Secret: Specifies the shared SPI secret between the PDSN service and the PCF. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default is MD5. A hash-algorithm is required for each SPI configured.
	Replay-protection process: Specifies how protection against replay-attacks is implemented. The possible processes are nonce and timestamp. The default is timestamp with a tolerance of 60 seconds. A replay-protection process is required for each SPI configured.
Subscriber session lifetime	Specifies the time in seconds that an A10 connection can exist before its registration is considered expired. The time is expressed in seconds and can be configured to any integer value between 1 and 65534, or the timer can be disabled to set an infinite lifetime. The default value is 1800 seconds.
Mobile IP FA context name	Specifies the name of the context in which the FA service is configured.

Required Information	Description
Default Subscriber Configuration	
"Default" subscriber's IP context name	Specifies the name of the egress context on the system that facilitates the PDN ports. **Important** For this configuration, the IP context name should be identical to the name of the destination context.

AAA Context Configuration

The following table lists the information that is required to configure the AAA context.

Table 8: Required Information for AAA Context Configuration

Required Information	Description
AAA context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the AAA context will be recognized by the system.
AAA Interface Configuration	
AAA interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. AAA interfaces will be configured in the source context.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.

Required Information	Description
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
Foreign/Home RADIUS Server Configuration	
Foreign/Home RADIUS Authentication server	IP Address: Specifies the IP address of the foreign/home RADIUS authentication server the source context will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers will be configured. Foreign/home RADIUS authentication servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the foreign/home RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.

Required Information	Description
Foreign/Home RADIUS Accounting server	IP Address: Specifies the IP address of the foreign/home RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured. Foreign/home RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the foreign/home RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the foreign/home RADIUS server. The name must be between 1 and 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the source context's AAA interface. A secondary IP address interface can optionally be configured.

Mobile IP Destination Context Configuration

The following table lists the information that is required to configure the destination context.

Table 9: Required Information for Destination Context Configuration

Required Information	Description
Mobile IP Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the Mobile IP destination context will be recognized by the system. **Important** For this configuration, the destination context name should **not** match the domain name of a specific domain. It should, however, match the name of the context in which the HA service is configured if a separate system is used to provide HA functionality.
ICC Interface Configuration	
ICC interface name	The intra-context communication (ICC) interface is configured to allow FA and HA services configured within the same context to communicate with each other. The ICC interface name is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. ICC interface(s) are configured in the same destination context as the FA and HA services.
IP address and subnet	These will be assigned to the ICC interface(s). Multiple addresses (at least one per service) on the same subnet will be needed to assign to the same ICC interface.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.

Required Information	Description
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical ICC interfaces.
PDN Interface Configuration	
PDN interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. PDN interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the PDN interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description(s)	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical PDN interfaces.
Gateway IP address(es)	Used when configuring static routes from the PDN interface(s) to a specific network.
IP Address Pool Configuration (optional)	

Required Information	Description
IP address pool name(s)	If IP address pools will be configured in the destination context(s), names or identifiers will be needed for them. The pool name can be between 1 and 31 alpha and/or numeric characters and is case sensitive.
IP pool addresses	An initial address and a subnet, or a starting address and an ending address, are required for each configured pool. The pool will then consist of every possible address within the subnet , or all addresses from the starting address to the ending address. The pool can be configured as public, private, or static.
FA Service Configuration	
FA service name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the FA service will be recognized by the system. Multiple names are needed if multiple FA services will be used. FA services are configured in the destination context.
UDP port number for Mobile IP traffic	Specifies the port used by the FA service and the HA for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 434.

Required Information	Description
Security Parameter Index (indices) Information	**HA IP address:** Specifies the IP address of the HAs with which the FA service communicates. The FA service allows the creation of a security profile that can be associated with a particular HA.
	Index: Specifies the shared SPI between the FA service and a particular HA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the FA service is to communicate with multiple HAs.
	Secrets: Specifies the shared SPI secret between the FA service and the HA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default is hmac-md5. A hash-algorithm is required for each SPI configured.
FA agent advertisement lifetime	Specifies the time (in seconds) that an FA agent advertisement remains valid in the absence of further advertisements. The time can be configured to any integer value between 1 and 65535. The default is 9000.
Number of allowable unanswered FA advertisements	Specifies the number of unanswered agent advertisements that the FA service will allow during call setup before it will reject the session. The number can be any integer value between 1 and 65535. The default is 5.
Maximum mobile-requested registration lifetime allowed	Specifies the longest registration lifetime that the FA service will allow in any Registration Request message from the mobile node. The lifetime is expressed in seconds and can be configured between 1 and 65534. An infinite registration lifetime can be configured by disabling the timer. The default is 600 seconds.

Required Information	Description
Registration reply timeout	Specifies the amount of time that the FA service will wait for a Registration Reply from an HA. The time is measured in seconds and can be configured to any integer value between 1 and 65535. The default is 7.
Number of simultaneous registrations	Specifies the number of simultaneous Mobile IP sessions that will be supported for a single subscriber. The maximum number of sessions is 3. The default is 1. **Important** The system will only support multiple Mobile IP sessions per subscriber if the subscriber's mobile node has a static IP address.
Mobile node re-registration requirements	Specifies how the system should handle authentication for mobile node re-registrations. The FA service can be configured to always require authentication or not. If not, the initial registration and de-registration will still be handled normally.
HA service Configuration	
HA service name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the HA service will be recognized by the system. Multiple names are needed if multiple HA services will be used. HA services are configured in the destination context.
UDP port number for Mobile IP traffic	Specifies the port used by the HA service and the FA for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 434.

Required Information	Description
Mobile node re-registration requirements	Specifies how the system should handle authentication for mobile node re-registrations. The HA service can be configured as follows: • Always require authentication • Never require authentication (**NOTE:** the initial registration and de-registration will still be handled normally) • Never look for mn-aaa extension • Not require authentication but will authenticate if mn-aaa extension present
FA-to-HA Security Parameter Index Information	**FA IP address:** The HA service allows the creation of a security profile that can be associated with a particular FA. This specifies the IP address of the FA that the HA service will be communicating with. Multiple FA addresses are needed if the HA will be communicating with multiple FAs.
	Index: Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.
	Secret: Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is hmac-md5. A hash-algorithm is required for each SPI configured.

Required Information	Description
Mobile Node Security Parameter Index Information	**Index:** Specifies the shared SPI between the HA service and the mobile node(s). The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple mobile nodes.
	Secret(s): Specifies the shared SPI secret between the HA service and the mobile node. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is hmac-md5. A hash-algorithm is required for each SPI configured.
	Replay-protection process: Specifies how protection against replay-attacks is implemented. The possible processes are nonce and timestamp. The default is timestamp with a tolerance of 60 seconds. A replay-protection process is required for each mobile node-to-HA SPI configured.
Maximum registration lifetime	Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node. The time is measured in seconds and can be configured to any integer value between 1 and 65535. An infinite registration lifetime can also be configured by disabling the timer. The default is 600.
Maximum number of simultaneous bindings	Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address. The number can be configured to any integer value between 1 and 5. The default is 3.
Default Subscriber Configuration	

Required Information	Description
"Default" subscriber's IP context name	Specifies the name of the egress context on the system that facilitates the PDN ports. **Important** For this configuration, the IP context name should be identical to the name of the destination context.

Simple IP Destination Context

The following table lists the information that is required to configure the optional destination context. As discussed previously, This context is only required if Reverse Tunneling is disabled in the FA service.

Table 10: Required Information for Destination Context Configuration

Required Information	Description
Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system. **Important** For this configuration, the destination context name should **not** match the domain name of a specific domain.
PDN Interface Configuration	
PDN interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. PDN interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the PDN interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.

Required Information	Description
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical PDN interfaces.
Gateway IP address(es)	Used when configuring static routes from the PDN interface(s) to a specific network.
IP Address Pool Configuration (optional)	
IP address pool name	Each IP address pool is identified by a name. The pool name can be between 1 and 31 alpha and/or numeric characters and is case sensitive. IP address pools are configured in the destination context(s). Multiple address pools can be configured within a single context.
IP pool addresses	An initial address and a subnet, or a starting address and an ending address, are required for each configured pool. The pool will then consist of every possible address within the subnet , or all addresses from the starting address to the ending address. The pool can be configured as public, private, or static.

System-Level AAA Parameter Configuration

The following table lists the information that is required to configure the system-level AAA parameters.

Table 11: Required Information for System-Level AAA Configuration

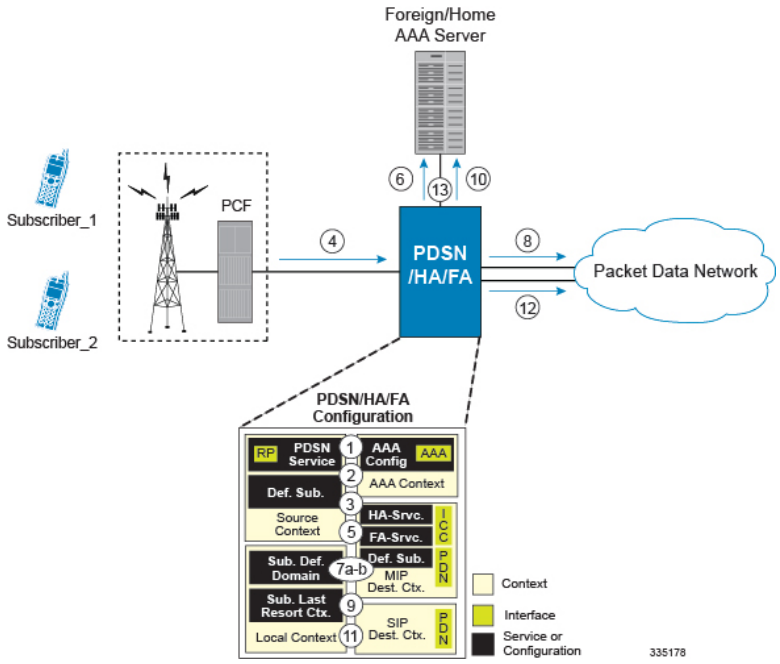
Required Information	Description
Subscriber default domain name	Specifies the name of a context that can provide AAA functions in the event that the domain-part of the username is missing or poorly formed. This parameter will be applied to all subscribers if their domain can not be determined from their username regardless of what domain they are trying to access. **Important** The default domain name can be the same as the source context.

Required Information	Description
Subscriber Last-resort context	Specifies the name of a context that can provide AAA functions in the event that the domain-part of the username was present but does not match the name of a configured destination context. This parameter will be applied to all subscribers if their specified domain does not match a configured destination context regardless of what domain they are trying to access. **Important** The last-resort context name can be the same as the source context.
Subscriber username format	Specifies the format of subscriber usernames as to whether or not the username or domain is specified first and the character that separates them. The possible separator characters are: • @ • % • - • \ • # • / Up to six username formats can be specified. The default is *username* @. **Important** The username string is searched from right to left for the separator character. Therefore, if there is one or more separator characters in the string , only the first one that is recognized is considered the actual separator. For example, if the default username format was used, then for the username string *user1@enterprise@isp1*, the system resolves to the username *user1@enterprise* with domain *isp1*.

How This Configuration Works

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a Simple IP data call.

Figure 11: Call Processing When Using the System as a PDSN, FA, and HA



In this example, *Subscriber1* is establishing a Simple IP data session, while *Subscriber2* is establishing a Mobile IP data session.

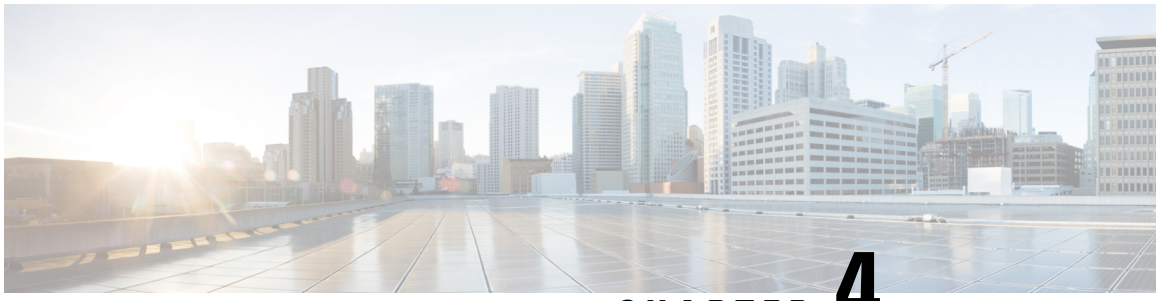
1. The system-level AAA settings were configured as follows:
   - Default domain name = *AAA*
   - Subscriber username format = *username @*
   - Last-resort context name = *AAA*
2. The Default Subscriber was configured with an IP context name of *SIP Destination.*
3. The Mobile IP FA context name parameter within the PDSN service was configured to the *MIP Destination* context.
4. Sessions for *Subscriber1* and *Subscriber2* are received by the PDSN service over the R-P interface from the PCF.
5. The PDSN service determines which context to use to provide foreign AAA functionality for each session. This process is described in the How the System Selects Contexts section located in the Understanding the System Operation and Configuration chapter of the *System Administration Guide*.

   For this configuration, the result of this process for both *Subscriber1* and *Subscriber2* would be that the system determines that AAA functionality should be provided by the *AAA* context.
6. The system would then communicate with the AAA server specified in the *AAA* context's AAA configuration to authenticate the subscribers.
7. Upon successful authentication, the PDSN service will take the following actions for *Subscriber1* and *Subscriber2*:

1. *Subscriber1*: The system will go through the process of determining which destination context to use for the subscriber session. This process is described in the How the System Selects Contexts section located in the Understanding the System Operation and Configuration chapter of the *System Administration Guide*. For this configuration, the system determines that the egress context is the *SIP Destination* context based on the configuration of the *Default* subscriber in the *Source* context.
2. *Subscriber2*: The system uses the Mobile IP FA context name configured within the PDSN service to determine what destination context facilitates the FA service. In this example, it determines that it must use the *MIP Destination* context and it passes the HA IP address to the FA service.

8. For *Subscriber1's session*, data traffic would then be routed through the PDN interface in the *SIP Destination* context.
9. For *Subscriber2*, the FA service then establishes a connection to the specified HA service through the ICC interface.
10. For *Subscriber2*, the system would then communicate with the AAA server specified in the *AAA* context\'s AAA configuration to authenticate the subscriber.
11. For *Subscriber2*, upon successful authentication, the *MIP Destination* context determines which destination context to use for the session and Mobile IP registration would be completed. This process is described in the How the System Selects Contexts section located in the Understanding the System Operation and Configuration chapter of the *System Administration Guide*.

    For this example, the *Source* context determines that the egress context is the *MIP Destination* context based on the configuration of the *Default* subscriber.
12. For *Subscriber2's session*, data traffic would then be routed through the PDN interface in the *MIP Destination* context.
13. Accounting messages for both sessions would be sent to the AAA server over the AAA interface in the *AAA* context.



CHAPTER 4

Service Configuration Procedures

This chapter is intended to be used in conjunction with the previous chapters that provide examples for configuring the system to support Simple IP services, Mobile IP services, or both. It provides procedures for configuring the various elements to support these services.

It is recommended that you first select the configuration example that best meets your service model, and then use the procedures in this chapter to configure the required elements for that model.

Note At least one packet processing card must be made active prior to service configuration. Information and instructions for configuring packet processing cards can be found in the "Configuring System Settings" chapter of the *System Administration Guide*.

Procedure are provided for the following:

- Creating and Configuring HA Services, on page 67
- Session Continuity Support, on page 69
- Hybrid HA Service Configuration, on page 71
- WiMAX-3GPP2 Interworking at HA, on page 73

Creating and Configuring HA Services

HA services are configured within contexts and allow the system to function as an HA in the 3G wireless data network.

To create and configure an HA service:

Step 1 Create and configure an HA service as described in the Creating and Configuring an HA Service, on page 68 section.

Step 2 Verify your configuration as described in the Verifying HA Service Configuration, on page 68 section.

Step 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. Additionally, when configuring Mobile IP take into account the MIP timing considerations discussed in the MIP Timer Considerations appendix.

Creating and Configuring an HA Service

Use the following example to configure HA services:

```
configure
 context <ha_context_name>
 ha-service <ha_service_name>
 ip local-port <port_number>
 authentication mn-aaa { allow-noauth | always | dereg-noauth | noauth |
 renew-and-dereg-noauth | renew-reg-noauth }
 fa-ha-spi remote-address <fa_ip_address> spi-number <number> { encrypted secret
 <enc_secret> | secret <secret> } [ description <string> ] [ hash-algorithm {
hmac-md5 | md5 | rfc2002-md5 } ]
               mn-ha-spi spi-number <number> [ description <string> ] {
encrypted secret <enc_secret> | secret <secret> } [ hash-algorithm { hmac-md5
 | md5 | rfc2002-md5 } ] [ permit-any-hash-algorithm ] [ replay-protection
 { nonce | timestamp } [ timestamp-tolerance <tolerance> ]
 reg-lifetime <lifetime>
 simul-bindings <simul_bindings>
 bind address <address> max-subscribers <max_subs>
 end
```

Notes:

- <*port_number*> must be the UDP port for the Pi interfaces\' IP socket.
- A maximum of 2048 FA-HA Security Parameter Index (SPI) can be configured for each HA service.
- <*lifetime*> must the longest registration lifetime that the HA service allows in any Registration Request message from the mobile node. An infinite registration lifetime can be configured using the **no reg-lifetime** command.
- Option: To configure the HA service for controlling the negotiation and sending of the I-bit in revocation messages, in the HA Service Configuration Mode, enter the following comand. By default, HA will not send I-bit in revocation message. **revocation negotiate-i-bit**
- Use the bind address command to bind the service to the Pi interface and specify the maximum number of subscribers that can access the service. The hardware configuration and features installed can affect the maximum subscriber sessions that can be supported.
- Option: To set the maximum period of time to set up a session, in the HA Service Configuration Mode, enter the following command: **setup-timeout** <*seconds*>
- Create and bind additional HA services to any other interfaces as required.

Verifying HA Service Configuration

Verify that your HA services were created and configured properly by entering the following command:

show ha-service { name service_name | all }

The output is a concise listing of HA service parameter settings similar to the following sample. In this sample, an HA service named ha1 was configured.

```
Service name:  ha1
  Context: ha
  Bind:                Done               Max Subscribers: 500000
  Local IP Address:    192.168.4.10 Local IP Port:   434
  Lifetime:            00h01m40s          Simul Bindings:  3
  Reverse Tunnel:      Enabled
  GRE Encapsulation with-key: Enabled   Keyless GRE Encapsulation: Disabled
  Optimize Tunnel Reassembly: Enabled    Setup Timeout:   60 sec
  Allow Priv Addr w/o Rev Tunnel: Disabled
  WIMAX-3GPP2 Interworking: Disabled
  SPI(s):
  MNHA: Remote Addr: 0.0.0.0             Description:
    Hash Algorithm:    HMAC_MD5          SPI Num:  258
    Replay Protection: Nonce             Timestamp Tolerance: 100
    Permit Any Hash Algorithm:    Enabled
  FAHA: Remote Addr: 195.20.20.6/32 Description:
    Hash Algorithm:    HMAC_MD5          SPI Num:  258
    Replay Protection: Timestamp         Timestamp Tolerance: 60
  'S' Lifetime Skew:   00h00m10s
  IPSEC AAA Context: aaa_context
  GRE Sequence Numbers: Disabled         GRE Sequence Mode: None
  GRE Reorder Timeout:  100 msec
  GRE Checksum:         Disabled         GRE Checksum Verification: Disabled
  Registration Revocation:    Disabled    Reg-Revocation I Bit: Enabled
  Reg-Revocation Max Retries: 3           Reg-Revocation Timeout: 3 (secs)
  Reg-Rev Handoff old-FA:     Enabled     Reg-Rev Idle-Timeout: Enabled
  Send NAI Extension in Reg-Revocation: Disabled
  MIP NAT Traversal: Disabled    Force UDP Tunnel: Enabled
  Default Subscriber:      None
  Max Sessions: 500000
  Service Status: Started
  MN-AAA Auth Policy:      Always
  MN-HA Auth Policy:       Always
  IMSI Auth:               Disabled
  DMU Refresh Key:         Disabled
  AAA Distributed MIP Keys:Disabled
  AAA accounting:          Enabled
  Idle Timeout Mode:       Aggressive
  Newcall Policy:          None
  Overload Policy:         Reject    (Reject code: Admin Prohibited)
  NW-Reachability Policy:  Reject    (Reject code: Admin Prohibited)
  Null-username Policy:    Reject
  BC Rsp Code for Nw Fail: 0xffff
  IP Pool/Group:
    Name: n/a
    Destination Context: n/a
```

Session Continuity Support

This section describes the procedure to enable the mobility for WiMAX subscriber and other access technology subscribers; i.e. 3GPP2. WiMAX HA implementation differs from 3GPP2 on the keys used to authenticate MN-HA and FA-HA AE in MIP RRQ. WiMAX HA involves using dynamic keys distributed by AAA for authenticating RRQ.

Following WiMAX support is provided for MIP keys management and WiMAX HA support:

- MIPv4 support
- Managing MIP Key distribution from AAA
- Registration Revocation
- MIPv4 RRQ with NAI extension
- Support of GRE key extension of CVSE in RRP
- MIPv4 Registration

For MIP registration HA uses the following extensions:

- MN-NAI Extension
- MN-HA AE
- Revocation Support Extension
- FA-HA AE

The MIP client includes the same NAI in all MIP RRQs it sends for the entire duration of the MIP session regardless of EAP re-authentication, including MIP renewal and de-registration messages. The MN-HA and FA-HA keys based on WiMAX VSA from AAA is used to authenticate the RRQ and compute authenticator in RRP.

Authentication algorithm used to authenticate MN-HA and FA-HA AE is HMAC-MD5. If renew/dereg RRQ is received, authentication with AAA will happen only if SPI value for authentication extension in RRQ changes. If SPI returned by AAA is different from the requested one, the RRQ will be rejected. Both MN-HA and FA-HA AE are expected in MIP RRQ for WiMAX calls.

The following describes the processing of different requests for HA support:

- Processing Access-Request: When initial MIP RRQ is received, HA authenticates with AAA to get the MIP Keys (MN-HA and HA-RK) required to authenticate MIP RRQ.
- Processing Access-Accept: In the Access Accept, MIP Keys MN-HA and HA-RK (if requested) is received. MN-HA key is maintained for each subscriber session and FA-HA key is computed based on HA-RK maintained per HA.

All the attributes (HA-RK-KEY, HA-RK-SPI, and HA-RK-Lifetime) must be returned if HA-RK key is requested for the HA-RK info in Access Accept to be valid.

Message Authenticator will be included in Access request and Accept packets for integrity protection of RADIUS packets and is mandatory.

- MIPv4 Revocation: MIP Revocation is supported as per RFC 3543 and it uses FA-HA keys fetched dynamically from AAA during MIP registration.

Apart from these processing, HA provides following function applicable to WiMAX HA.

- Functional Level Description: HA retrieves the MIP Keys dynamically from AAA to authenticate the RRQ.
- Authentication of MIP RRQ in WiMAX HA: When a MIP RRQ is received HA authenticates the user with AAA for both P-MIP and C-MIP call to get the MIP Keys.

The MN-HA and FA-HA keys will be used to authenticate the RRQ.

Hybrid HA Service Configuration

With this support an HA can work in a "hybrid" mode, meaning the same HA can handle a call from CDMA network, a call from WIMAX network, and a "hybrid call" with RRQ coming from one network and later from another network. This way, the operator can just deploy one HA service to support both types of network, instead of using two separate HA services. The HA is aware of the access technology, and choose the correct authentication method to handle RRQ.

This section describes the following configuration procedures:

- Configuring WiMAX HA for WiMAX Calls only, on page 71
- Configuring WiMAX HA to Accept 3GPP2/Static MIP Key, on page 72
- Configuring Hybrid HA for WiMAX and 3GPP2 Calls, on page 72

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 WiMAX HA for WiMAX Calls only

With this configuration the system will support only WiMAX HA behavior for the particular HA-service, where the system always expects WiMAX MIP keys from AAA and use it to do MN-HA and FA-HA authentication extension. With this configuration HA cannot support calls with static keys for MIP RRQ authentication in the particular HA service.

To configure WiMAX HA for WiMAX calls only:

Step 1 Configure WiMAX HA for WiMAX calls only as described in this section.

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*.

Use the following example to configure WiMAX HA services, and enable the usage of AAA provided WiMAX MIP keys for authenticating MIP RRQ with keys mandatory.

```
configure
 context <ha_context_name>
 ha-service <ha_service_name>
 authentication aaa-distributed-mip-keys required
 end
```

Configuring WiMAX HA to Accept 3GPP2/Static MIP Key

To configure WiMAX HA to accept 3GPP2/Static MIP key:

Step 1 Configure WiMAX HA to accept 3GPP2/Static MIP key as described in this section.

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*.

Use the following example to configure HA services to accept 3GPP2 calls and disable usage of AAA provided WiMAX MIP keys for authenticating MIP RRQ.

```
configure
 context <ha_context_name>
 ha-service <ha_service_name>
 authentication aaa-distributed-mip-keys disabled
 end
```

Configuring Hybrid HA for WiMAX and 3GPP2 Calls

With this configuration, both WiMAX and 3GPP2 based calls can be made where WiMAX based calls will use WiMAX MIP keys, and 3GPP2 calls can use static or 3GPP2 based dynamic keys. This particular HA service configuration supports calls of both access technologies.

To configure Hybrid HA for WiMAX and 3GPP2 calls:

Step 1 Configure Hybrid HA to accept WiMAX and 3GPP2 calls in the same service as described in this section.

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*.

Use the following example to configure HA services to accept WiMAX and 3GPP2 calls in the same service, and enable usage of AAA provided WiMAX MIP keys for authenticating MIP RRQ with fallback option to use 3GPP2/static keys:

```
configure
 context <ha_context_name>
 ha-service <ha_service_name>
 authentication aaa-distributed-mip-keys optional
 wimax-3gpp2 interworking
 end
```

WiMAX-3GPP2 Interworking at HA

The session continuity capability enables a dual mode device (a multi radio device) to continue its active data session as it changes its active network attachment from 3GPP2 to Wimax and vice versa with no perceived user impacts from a user experience perspective.

This capability provides the following benefits:

- common billing and customer care
- accessing home 3GPP2 service through Wimax network and vice versa
- better user experience with seamless session continuity

To provide this capability, the HA supports seamless handoff from 3GPP2 to WIMAX and vice versa.

This section describes the key configuration to enable this capability.

Mobile Node Requirement

Following are the mandatory functional requirements on mobile node to support 3GPP2-WIMAX Interworking at HA:

- The dual mode MS SHOULD use PMIP to access WIMIAX network and use CMIP to access 3GPP2 network.
- The static NAI (the NAI that is pre-provisioned for access to 3GPP2) has to be used in RRQ on both 3GPP2 and WiMAX networks.
- The dual mode MS SHOULD support "make-before-break" when changing between 3GPP2 and WiMAX networks, if coverage is available on both networks.
- The CMIP4 RRQ message used on 3GPP2 network MUST contain the MN-AAA and Foreign Agent Challenge Extension (FACE)

H-AAA Requirements

H-AAA MUST meets the following requirements to support 3GPP2-WIMAX Interworking at HA:

- The H-AAA servers used by 3GPP2 and WIMAX SHOULD be either the same or they have access to the same session state and subscriber profile.
- H-AAA server SHOULD assign and return the same HA address in response to 3GPP2 and WIMAX network access request

FA and HA Function for 3GPP-WiMAX Interworking at HA

The FA and PMIP4 client provides following functionality to support 3GPP2-WIMAX Interworking at HA:

- For WiMAX access, the PMIP4 Client will NOT include MN-AAA AE in the RRQ.

- For 3GPP2 access, the FA will NOT remove the MN-AAA AE from the RRQ. This requirement stands even if the cdma2000 AAA sends the MN-AAA Removal Indication VSA with its value set.

The HA provides following functionality to support 3GPP2-WIMAX Interworking at HA:

- The HA recognizes the difference between 3GPP2 and WiMAX access technologies based on the presence or absence of MN-FA and MN-AAA AE. If the MN-FA and MN-AAA are present in the RRQ, the HA assumes that the RRQ is coming through a 3GPP2 network. Otherwise, the HA assumes that the RRQ is coming through a WiMAX network.
- The HA updates mobility bindings for different access technology types while maintaining binding integrity (binding continues to be active until updated).
- The same HA is able to handle packets from the MS with a given Care-of Address when the mobility binding is pointing to a different Care-of Address. This is to mitigate packet loss in the uplink during seamless mobility across access technologies.

Before configuring the 3GPP-WiMAX Interworking the following must be taken into consideration:

- Separate FA service is used for 3GPP2 and WIMAX network.
- The subscriber MUST be authorized to use PMIP for WIMAX access.
- The subscriber MUST use CMIP to access 3GPP2 network and MUST NOT set s-bit in RRQ.

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 WiMAX FA Service

To configure WiMAX FA service:

Step 1 Configure WiMAX FA service as described in this section.

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*.

Use the following example to configure WiMAX FA service:

```
configure
  <context_name>
context
 fa-service <fa_service_name>
 authentication aaa-distributed-mip-keys override
 revocation negotiate-i-bit
 end
```

Configuring 3GPP2 FA Service

To configure 3GPP2 FA service:

Step 1 Configure 3GPP2 FA service as described in this section.

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*.

Use the following example to create and configure 3GPP2 FA service:

```
configure
 context <context_name>
 fa-service <fa_service_name>
 default mn-aaa-removal-indication
 revocation negotiate-i-bit
 end
```

Important Notes:<*fa_service_name*> must be the FA service designated for 3GPP2 service.

Configuring Common HA Service

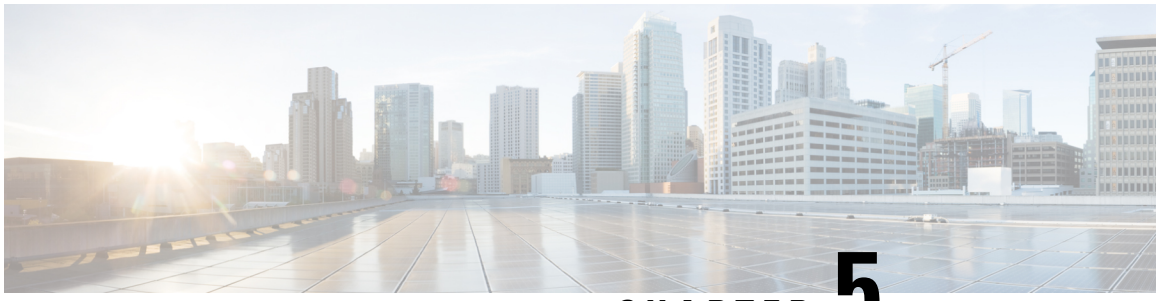
To configure common HA service:

Step 1 Configure common HA service as described in this section.

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*.

Use the following example to configure common HA service:

```
configure
 context <ha_context_name>
 ha-service <ha_service_name>
 authentication aaa-distributed-mip-keys required
 wimax-3gpp2 interworking
 authentication mn-aaa allow-noauth
 revocation negotiate-i-bit
 end
```



CHAPTER 5

Monitoring the Service

This chapter provides information for monitoring service status and performance using the **show** commands found in the Command Line Interface (CLI). These command have many related keywords that allow them to provide useful information on all aspects of the system ranging from current software configuration through call activity and status.

The selection of keywords described in this chapter is intended to provided the most useful and in-depth information for monitoring the system. For additional information on these and other **show** command keywords, refer to the *Command Line Interface Reference*.

In addition to the CLI, the system supports the sending of Simple Network Management Protocol (SNMP) traps that indicate status and alarm conditions. Refer to the *SNMP MIB Reference Guide* for a detailed listing of these traps.

Monitoring System Status and Performance

This section contains commands used to monitor the status of tasks, managers, applications and other software components in the system. Output descriptions for most of the commands are located in the *Counters and Statistics Reference.*

Important Not all Show commands are available for all platforms and licenses.

Table 12: System Status and Performance Monitoring Commands

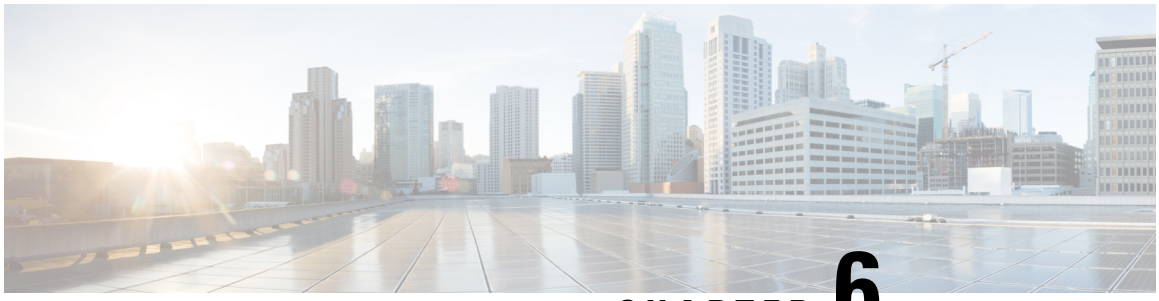
To do this:	Enter this command:
View HA Manager statistics	**show session subsystem facility hamgr all**
View Mobile IP Home Agent Statistics	
Display Mobile IP HA Information for a Specific Subscriber	
View Mobile IP HA information and counters for a specific subscriber	**show mipha full username** *subscriber_name*
Display Mobile IP Statistics for HA Services	

To do this:	Enter this command:
View Mobile IP statistics for a specific HA service	**show mipha statistics ha-service** *service_name*
Display Mobile IP HA Counters	
View Mobile IP HA counters for individual subscriber sessions	**show mipha counters**

Clearing Statistics and Counters

It may be necessary to periodically clear statistics and counters in order to gather new information. The system provides the ability to clear statistics and counters based on their grouping (PPP, MIPHA, MIPFA, etc.).

Statistics and counters can be cleared using the CLI **clear** command. Refer to the *Command Line Interface Reference* for detailed information on using this command.



CHAPTER 6

Engineering Rules

This section provides engineering rules or guidelines that must be considered prior to configuring the system for your network deployment.

Interface and Port Rules

The rules discussed in this section pertain to both the Ethernet 10/100, the Ethernet 1000 Line Card and the four-port Quad Gigabit Ethernet Line Card, known as the Quad Gig-E or QGLC and the type of interfaces they facilitate, regardless of the application.

Pi Interface Rules

HA to FA

The following engineering rules apply to the Pi interface between the HA and FA:

- When supporting Mobile IP, the system can be configured to perform the role of a FA, an HA or both. This section describes the engineering rules for the Pi interface when using the system as an HA.
- A Pi interface is created once the IP address of a logical interface is bound to an HA service.
- The logical interface(s) that will be used to facilitate the Pi interface(s) must be configured within an ingress context.
- HA services must be configured within an ingress context.
- If the system configured as an HA is communicating with a system configured as a FA, then it is recommended that the name of the context in which the HA service is configured is identical to the name of the context that the FA service is configured in on the other system.
- Each HA service may be configured with the Security Parameter Index (SPI) of the FA that it will be communicating with over the Pi interface.

- Multiple SPIs can be configured within the HA service to allow communications with multiple FAs over the Pi interface. It is best to define SPIs using a netmask to specify a range of addresses rather than entering separate SPIs. This assumes that the network is physically designed to allow this communication.
- Each HA service must be configured with a Security Parameter Index (SPI) that it will share with mobile nodes.
- Depending on the services offered to the subscriber, the number of sessions facilitated by the Pi interface can be limited in order to allow higher bandwidth per subscriber.

Subscriber Rules

The following engineering rule applies to subscribers configured within the system:

Default subscriber templates may be configured on a per HA service.

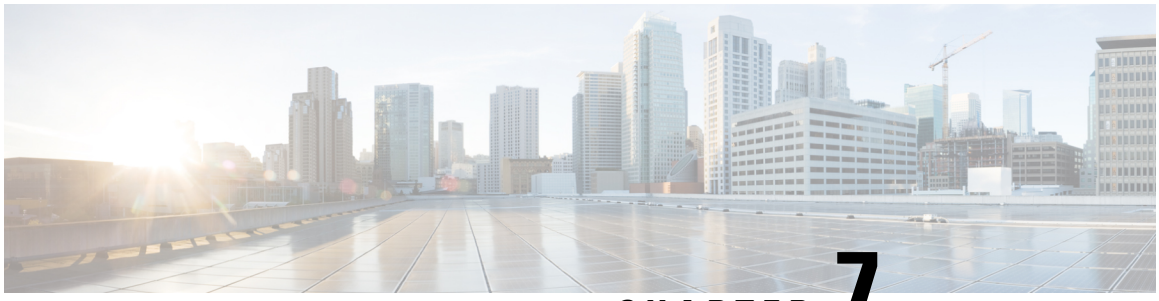
Service Rules

The following engineering rules apply to services configured within the system:

Important Given capacities do not apply to the XT2 platform.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

- A maximum of 256 services (regardless of type) can be configured per system.
- Up to 2,048 MN-HA and 2048 FA-HA SPIs can be supported for a single HA service.
- Up to 2,048 FA-HA SPIs can be supported for a single FA service.
- The system supports unlimited peer FA addresses per HA.
  - The system maintains statistics for a maximum of 8192 peer FAs per HA service.
  - If more than 8192 FAs are attached, older statistics are identified and overwritten.
- The system maintains statistics for a maximum of 4096 peer HAs per FA service.
- There are a maximum of 8 HA assignment tables per context and per chassis.
- The total number of entries per table and per chassis is limited to 256.
- Single HA service shall support more than one enterprise.
- Total number of service addresses per VPN context limited to 512.



CHAPTER 7

Supported Registration Reply Codes

The following section describes the registration reply codes supported by the system for the HA service.

• HA Service Reply Codes, on page 81

HA Service Reply Codes

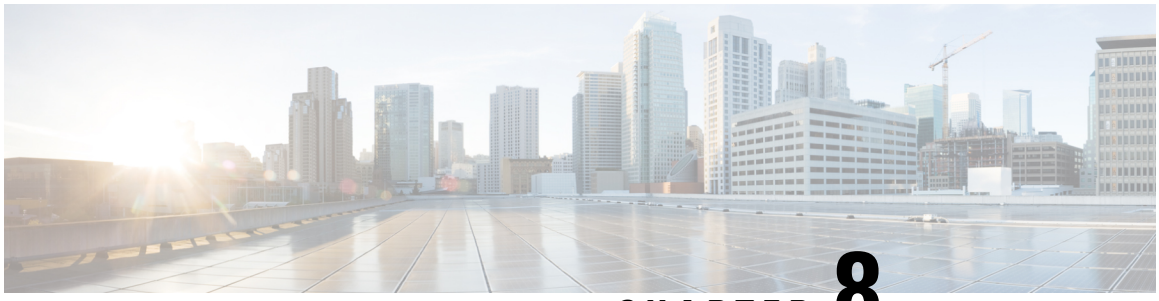
The following registration reply codes are supported by the system\'s HA service in accordance with the following Request For Comments (RFCs):

- RFC-2002, IPv4 Mobility, May 1995
- RFC-2344, Reverse Tunneling for Mobile IP, May 1998

Table 13: Supported HA Service Registration Reply Codes

Reply Code (Hex / Base 10)	Description	Note
80H / 128	Registration Denied - reason unspecified	Sent when internal errors are encountered when processing the Request packet.
81H / 129	Registration Denied - administratively prohibited	Sent when a newcall policy is set to reject calls or the subscriber is not permitted to use Mobile IP HA services.
82H / 130	Registration Denied - insufficient resources	Sent when no memory or session managers are available to process the session.
83H / 131	Registration Denied - mobile node failed authentication	Sent when the mobile node failed authentication.
84H / 132	Registration Denied - foreign agent failed authentication	Sent when an FA attempted to communicate with the HA service using an incorrect security parameter index (SPI).

Reply Code (Hex / Base 10)	Description	Note
85H / 133	Registration Denied - registration Identification mismatch	Sent when the ID sent by the mobile node in the RRQ is different from the expected value.
86H / 134	Registration Denied - poorly formed request	Sent when the registration request is poorly formed (i.e. missing an Authentication extension).
87H / 135	Registration Denied - too many simultaneous mobility bindings	Sent when the mobile node has exceeded the maximum number of mobile bindings that the HA service supports for a single subscriber.
88H / 136	Registration Denied - unknown home agent address	Sent when HA redirect policy is invoked.
89H / 137	Registration Denied - reverse tunneling unavailable	Sent when reverse tunneling is requested by the mobile node but it is not enabled on the system.
8AH / 138	Registration Denied - reverse tunneling mandatory	Sent when reverse tunneling is enabled on the system but is not supported by the mobile node.
8BH / 139	Registration Denied - reverse tunneling encapsulation style unavailable	Sent if the Encapsulating Delivery Style Extension sent by the mobile is not supported by the HA service.
8DH / 141	Registration Denied - unsupported Vendor-ID or unable to interpret Vendor-CVSE-Type.	Sent if the Vendor Identification is unsupported or the HA is unable to interpret the Vendor-CVSE-Type in the CVSE sent by the Foreign Agent to the Home Agent.
8EH / 142	Registration Denied - Requested UDP tunnel encapsulation unavailable	Sent by the HA if a UDP tunneling mode is not available.



CHAPTER 8

Mobile-IP and Proxy-MIP Timer Considerations

This section is intended to provide a brief explanation of the considerations for lifetime, idle, and absolute timer settings that must be understood when setting up a system in a mobile IP or proxy mobile IP environment. In the Cisco ASR 5500 platform, there is not an explicitly defined MIP lifetime. The MIP lifetime is determined through various timers settings in the configuration and through radius attributes returned in an Access-Accept message.

This chapter contains the following topics:

Call Flow Summary

The following steps describe the call flow as regards the timers that affect a call initiated by the Mobile Node (MN).

1. **PPP Negotiation**: A data call is initiated by beginning PPP. Once PPP is successfully established, the system will understand if the call is a mobile IP call or simple IP call. At this point, the system is not aware of the subscriber username and will use settings from the default subscriber template in the source context or the context defined by the "aaa default-domain subscriber" setting in the global configuration.
2. **FA Agent Advertisement**: Once the system has determined the call is a Mobile IP call, the FA will send a Router Advertisement message with a Mobility Agent Advertisement extension. The Mobility Agent Advertisement includes a Registration Lifetime field. The value of this field will come from one of two places. The FA service has a configurable setting named "advertise reg-lifetime". The default value for this setting is 600. A setting in the default subscriber template called "timeout idle" is also a candidate. The default value for this setting is 0 (null). The smaller of these two configurable parameters is used as the Registration Lifetime value. Leaving the settings at the defaults will result in an advertised lifetime of 600.

Advertise Reg-Lifetime in FA Service	Timeout Idle in Subscriber Template	Resulting Advertised Registration Lifetime
600	0	600
600	900	600
3600	1200	1200

The device will receive the agent advertisement and send a MIP Registration Request. The device uses the advertised registration lifetime value as the requested MIP lifetime.

3. **AAA Authentication and MIP Registration Request**: The next step in the MIP process will be to authenticate the user at the FA. It is at this stage where a failure condition can be introduced.

   If the Access-Accept message does not return any values related to timers, the subscribers MIP Registration Request is sent on to the HA.

   If the Access-Accept message does include an attribute relating to Idle or Absolute timer the FA will evaluate the requested lifetime from the device to the value returned by the AAA. The FA will treat any Idle or Absolute timer value returned by the AAA as a maximum value and as such:

   - If the requested MIP lifetime from the device is less-than than the returned radius attribute, the lifetime value is considered valid and the MIP Registration Request is forwarded on to the HA.
   - If the requested MIP lifetime from the device is greater-than the returned radius attribute, the requested lifetime value is considered to be too long. The FA will send a MIP Registration Reply to the device with a response code of Error 69 - Requested Lifetime Too Long. In the reply message, the FA will populate the Lifetime value with the maximum acceptable lifetime. The device may send a new MIP request with this new lifetime value.

MIP Lifetime Requested by Device	Idle-Timer Value in Access-Accept	Resulting MIP Lifetime Request in MIP Request to HA
3600	(Not Returned)	3600
3600	7200	3600
3600	1800	Failure - Error 69

4. **HA Process MIP Request**: The HA has now received a Mobile IP Registration request forwarded by the FA on behalf of the device. The MIP request contains the username and the requested lifetime (as well as other parameters). The HA will take this lifetime request and compare it to the configurable parameters associated with the HA service and associated configurations. The HA will use the username to determine which subscriber template to use for subscriber specific settings.

   The parameters the HA uses to determine the MIP lifetime are the requested lifetime, the "reg-lifetime" setting in the HA service and the "timeout idle" setting in the subscriber template. If the requested MIP lifetime is lower it is be sent back to the mobile; if the MIP lifetime is higher the system sends back an RRQ accept with the lifetime set to 5 seconds less than the lower of the idle or absolute timeout for the user.

MIP Lifetime Requested by Device	Timeout Idle/Absolute in Subscriber Template	Reg-Lifetime Value in HA Service	MIP Lifetime Returned to Mobile Device
3600	0(default)	7200	3600
3600	7200	1805	1800
3600	1705	3600	1700

PDSN/FA			HA		
Advertise Reg-Lifetime in FA Service	**Timeout Idle/Absolute in Subsc. Template (Source Context)**	**Idle-Timer Value in Access-Accept**	**Timeout Idle/Absolute in Subscriber Template(HA Context)**	**Reg-Lifetime Value in HA Service**	**Resulting Lifetime Value sent to Mobile Device**
600	0(default)	(not returned)	0(default)	7200	600
1800	900	7200	7200	1805	900
3600	1200	3600	1705	3600	1200
1500	3600	1500	0(default)	3600	1500
3600	0(default)	(not returned)	0(default)	2405	2400
3600	0(default)	(not returned)	2005	3600	2000
65534	0(default)	7200	0(default)	3600	Lifetime Too Long

Dealing with the 'Requested Lifetime Too Long' Error Code

In some configurations, a roaming partner may return an "Idler-Timer" attribute in an access-accept whose value is smaller than what a carrier may have configured for its own subscribers. This will result in a "Requested Lifetime Too Long" error message being returned to the device. There are several ways to correct this. One is to use a setting in the FA service configuration. Using the "no limit-reg-lifetime" in the FA service configuration will tell the FA service to allow the MIP lifetime to be greater than the Idle or Absolute timers. The FA will not send Error 69 and continue to process the call. The lifetime value in the MIP Request sent to the HA will still be what was determined in Phase 2.

Controlling the Mobile IP Lifetime on a Per-Domain Basis

The system does not support the configuration of the MIP lifetime timer on per- domain (context) basis. However, a domain-wide lifetime timer can be achieved by configuring the idle-timeout attribute for the default subscriber for each domain.

Important Mobile IP lifetime settings can be controlled on a per-domain basis **only** in deployments for which the idle timeout attribute for individual subscriber profiles is **not** used during operation.

In this configuration, the value of the registration lifetime sent by the system in Agent Advertisements is selected by comparing the configured FA Agent Advertisement lifetime setting, and the idle and/or absolute timeout settings configured for the domain\'s default subscriber. If the value of the idle and/or absolute timeout parameter is less than the Agent Advertisement lifetime, then the system provides a registration lifetime equal to 5 seconds less than the lowest timer value.

If the idle timeout attribute is configured in individual subscriber profiles, per-domain lifetime control is not possible. In this case, the registration lifetime configured for the FA must be the lower of the two values.

Important Commands used in the 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.

The following is an example CLI command sequence used to configure the Mobile IP lifetime on a per-domain basis.

```
configure
     context <aaa_context_name>
          subscriber default
               ip context-name <abc>
               exit
          subscriber name <ptt.bigco.com>
               timeout idle <3605>
               ip context-name <abc>
               exit
          subscriber name <bigco.com>
               timeout idle <7205>
               ip context-name <abc>
               exit
          domain <ptt.bigco.com> default subscriber <ptt.bigco.com>
          domain <bigco.com> default subscriber <bigco.com>
               end
configure
     context <ha_context_name>
          subscriber default
          exit
     ha-service <ha>
          idle-timeout-mode normal
          reg-lifetime <7200>
          end
configure
     context <fa_context_name>
          fa-service <fa>
               advertise reg-lifetime <7200>
               end
```

In the example above, two domains (ptt.bigco.com and bigco.com) are configured. The default subscribers are defined for the two domains respectively. The desired operation requires a Mobile IP lifetime of 1 hour (3600 secs) for the ptt.bigco.com domain, and a lifetime of 2 hours (7200 secs) for the bigco.com domain.

Whenever a subscriber session belonging to the ptt.bigco.com domain arrives, the system uses a Mobile IP lifetime timer value equal to 5 seconds less than the idle timeout configured for the default subscriber because the configured value is less than the registration lifetime value configured for the Agent Advertisement. 5 seconds less than the configured value of 3605 seconds equals 3600 seconds which meets the desired operation.

Whenever a subscriber session belonging to the bigco.com domain arrives, the system uses the configured registration lifetime value as the Mobile IP lifetime in Agent Advertisements because it is less than the configured idle timeout in the default subscriber\'s profile.

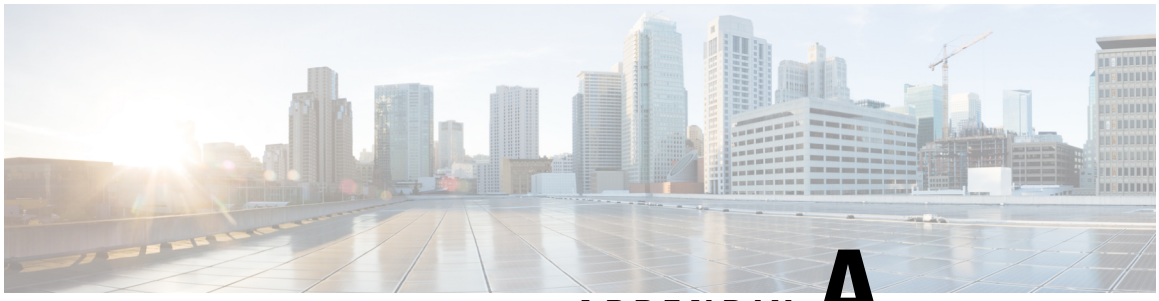
As a general rule, the registration lifetime value on the agent **must** be configured as the highest Mobile IP lifetime that is desired for a subscriber. (In the above example, it would be the subscriber bigco.com.)

Another important factor to consider is that the idle timeout value should be reset on receipt of a renewal request. To support this operation, the system provides the **idle-timeout-mode** configurable in the HA service. The following modes are supported:

- **normal**: Resets the idle timeout value on receipt of Mobile IP user data and control signaling
- **aggressive**: Resets the idle timeout value on receipt of Mobile IP user data only (this is the default behavior)
- **handoff**: Resets the idle timeout value on receipt of Mobile IP user data and upon inter-AGW handoff or inter access technologies

The following optional modifier is also supported:

- **upstream-only**: Only upstream user data (data from the mobile node) resets the idle timer for the session. This is disabled by default.



APPENDIX A

Always-on

This chapter provides information on configuring an enhanced, or extended, service. 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.

This chapter contains the following topics:

Overview

Always-on is enabled for each subscriber individually through a local subscriber profile or a RADIUS profile. Always-on is disabled for all subscribers by default.

If Always-on is enabled for a subscriber, when the idle time-out limit is reached the subscribers IP/PPP session remains connected as long as the subscriber is reachable. This is true even if the airlink between the mobile device and the RN (Radio Node) is moved from active to dormant (inactive) status. When the idle timeout limit is reached, the PDSN determines Mobile Node availability using LCP keepalive messages. A response to these messages indicates that the "always-on" status should be maintained. Failure to respond to a predetermined number of LCP keepalive messages causes the PDSN to tear-down (disconnect) the subscriber session.

Caution When always-on is enabled, the subscriber must have an idle time-out period configured (default is 0, no time-out). Failure to configure an idle time-out results in the LCP keepalive messages never being sent and the subscriber session stays up indefinitely.

The RADIUS attribute **3GPP2-Always-On** defined in a subscriber profile stored remotely on a RADIUS server can be used to enable Always-on for the subscriber. The attribute has two possible values, **inactive** and **active**. To enable Always-on, set the attribute to **active**.

For more information on the attributes, if you are using StarOS 12.3 or an earlier release, refer to 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*.

Configuring Always-on

To configure Always-on for a subscriber:

Step 1 Configure Always-on as described in the Configuring Always-on, on page 90.

Step 2 Verify your configuration as described in the Verifying Your Configuration, on page 91.

Step 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*.

What to do next

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 Always-on

Use the following example to configure Always-on:

```
configure
     context <context_name>
          subscriber name <subscriber_name>
          timeout idle <seconds>
          always-on
          end
```

Notes:

- <*context_name*> must be the name of the destination context where the subscriber that you want to enable always-on is configured.
- *Option:* To configure the echo-retransmit-timeout setting to wait before sending a keepalive message to an always-on subscriber, in the Context Configuration Mode, enter the following command:

  ppp echo-retransmit-timeout <*milliseconds*>

- *Option:* To configure the echo-max-retransmissions setting to retransmit a Keepalive message to a subscriber, in the Context Configuration Mode use the following command:

  ppp echo-max-retransmissions <*num_retries*>

- The optional echo-retransmit-timeout and echo-max-retransmissions settings apply to all subscriber sessions within the current context that have always-on enabled.
- *Option:* To configure the long duration timer for the subscriber, in the Subscriber Configuration Mode, enter the following command:

timeout long-duration <*ld_timeout*> **[inactivity-time** <*inact_timeout*>**]**

- *Option:* To configure the long duration timer detection to trigger long duration timer action for the subscriber, in the Subscriber Configuration Mode enter the following command:

  long-duration-action detection

- *Option:* To configure the long duration timer action for sessions exceeding the long duration timer timeout or the idle timeout durations for the subscriber, in the Subscriber Configuration Mode enter the following command:

  long-duration-action disconnection [suppress-notification] [dormant-only] +

Verifying Your Configuration

To verify your configuration:

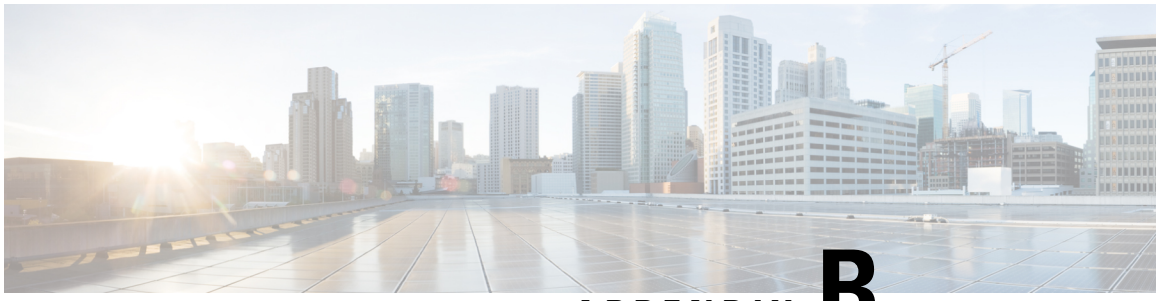
Step 1 Change to the context where Always-on was configured by entering the following command:

`context` *`<context_name>`*

Step 2 View the subscriber\'s configuration by entering the following command:

`show subscriber configuration username` *`<name>`*

Output of the command displays the subscriber\'s configurations. Examine the output for the idle timeout and always-on fields.



APPENDIX B

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 94.

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 97.

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 **readdress 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 93.

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:

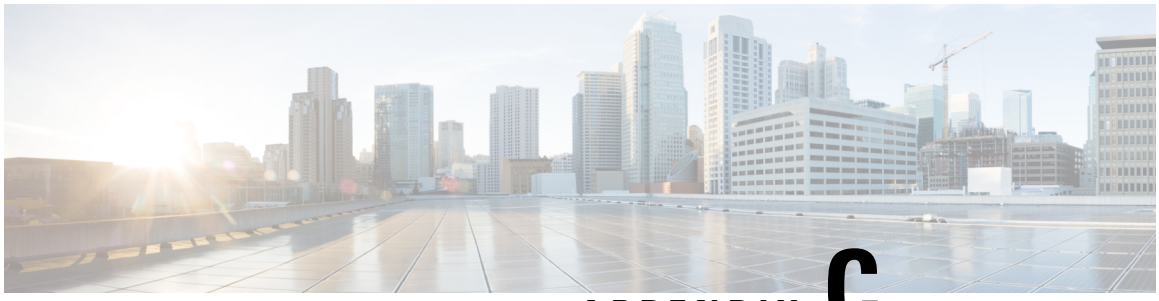
```
username: user1 callid: 01ca11b1    msid: 0000100003
  Card/Cpu: 4/2
  Sessmgr Instance: 7
  Primary callline:
  Redundancy Status: Original Session
  Checkpoints   Attempts    Success    Last-Attempt   Last-Success
     Full:            27         26         15700ms        15700ms
     Micro:  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

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

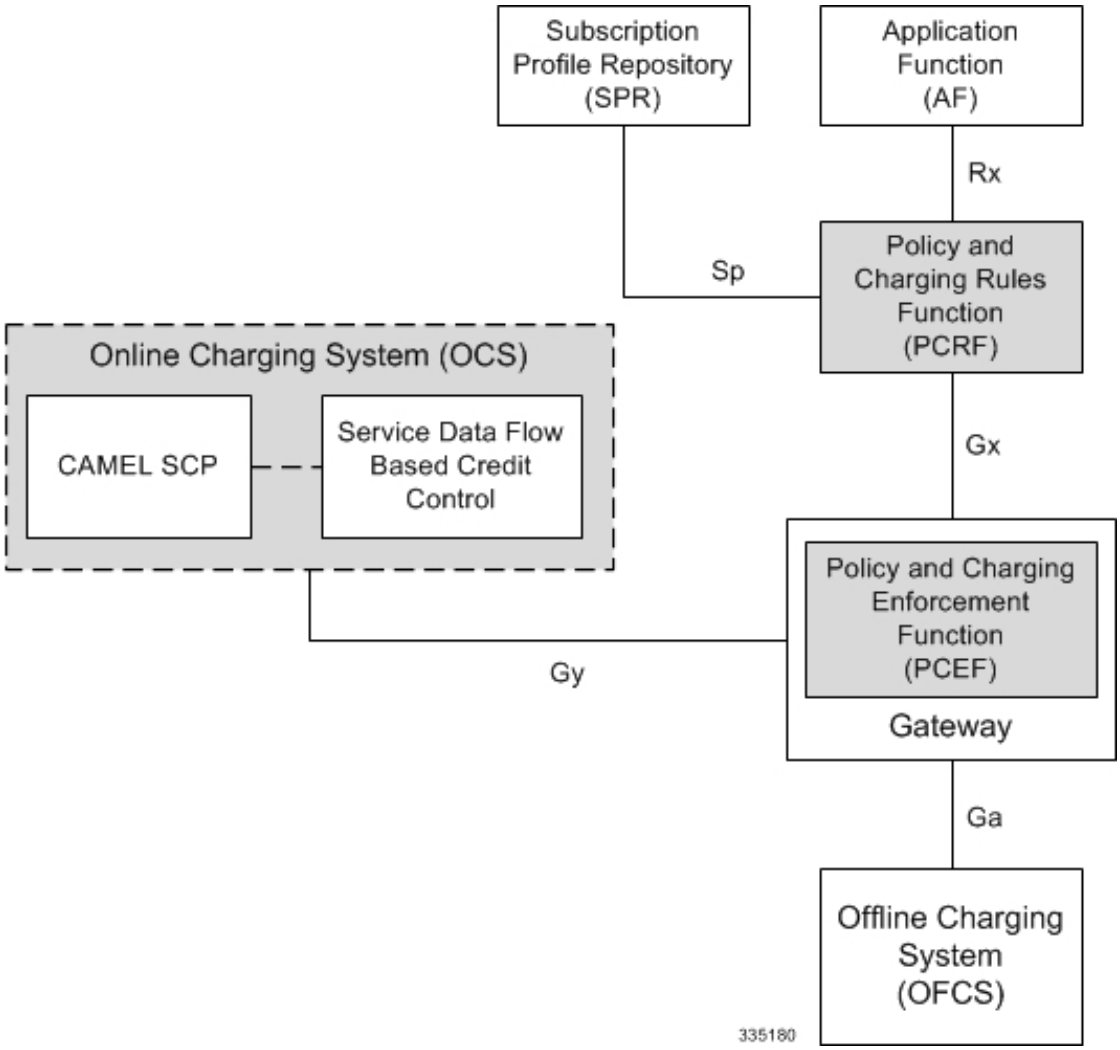
For IMS deployment in GPRS/UMTS networks the system uses Rel. 7 Gx interface for policy-based admission control support and flow-based charging. The Rel. 7 Gx interface supports enforcing policy control features like gating, bandwidth limiting, and so on, and also supports flow-based charging. This is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

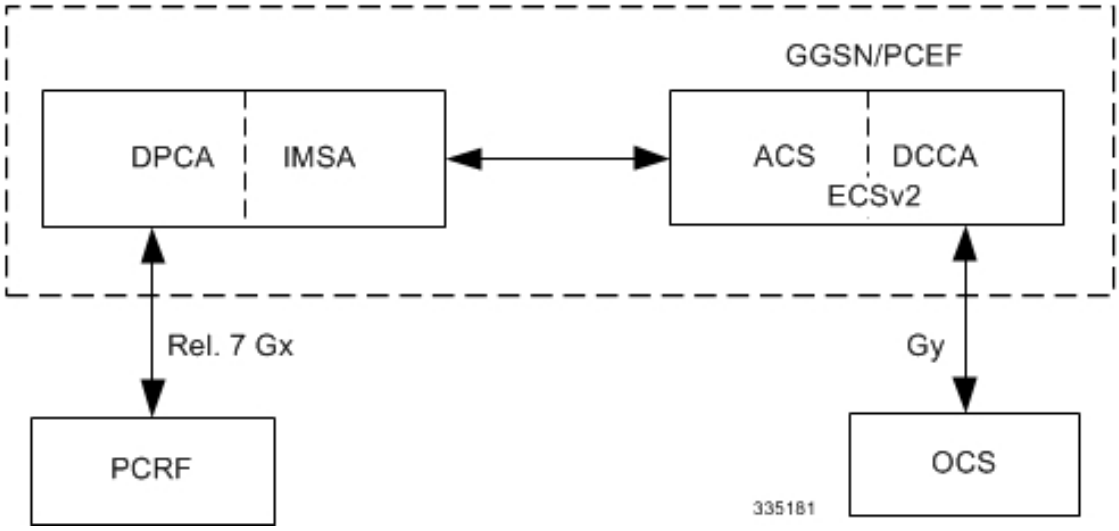
The Rel. 7 Gx reference point is located between the Gateway and the PCRF. This reference point is used for provisioning and removal of PCC rules from the PCRF to the Gateway, and the transmission of traffic plane events from the Gateway to the PCRF. The Gx reference point can be used for charging control, 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 12: 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 13: 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

Gx Interface Support

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 129.

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 14: Rel. 7 Gx IMS Authorization Call Flow

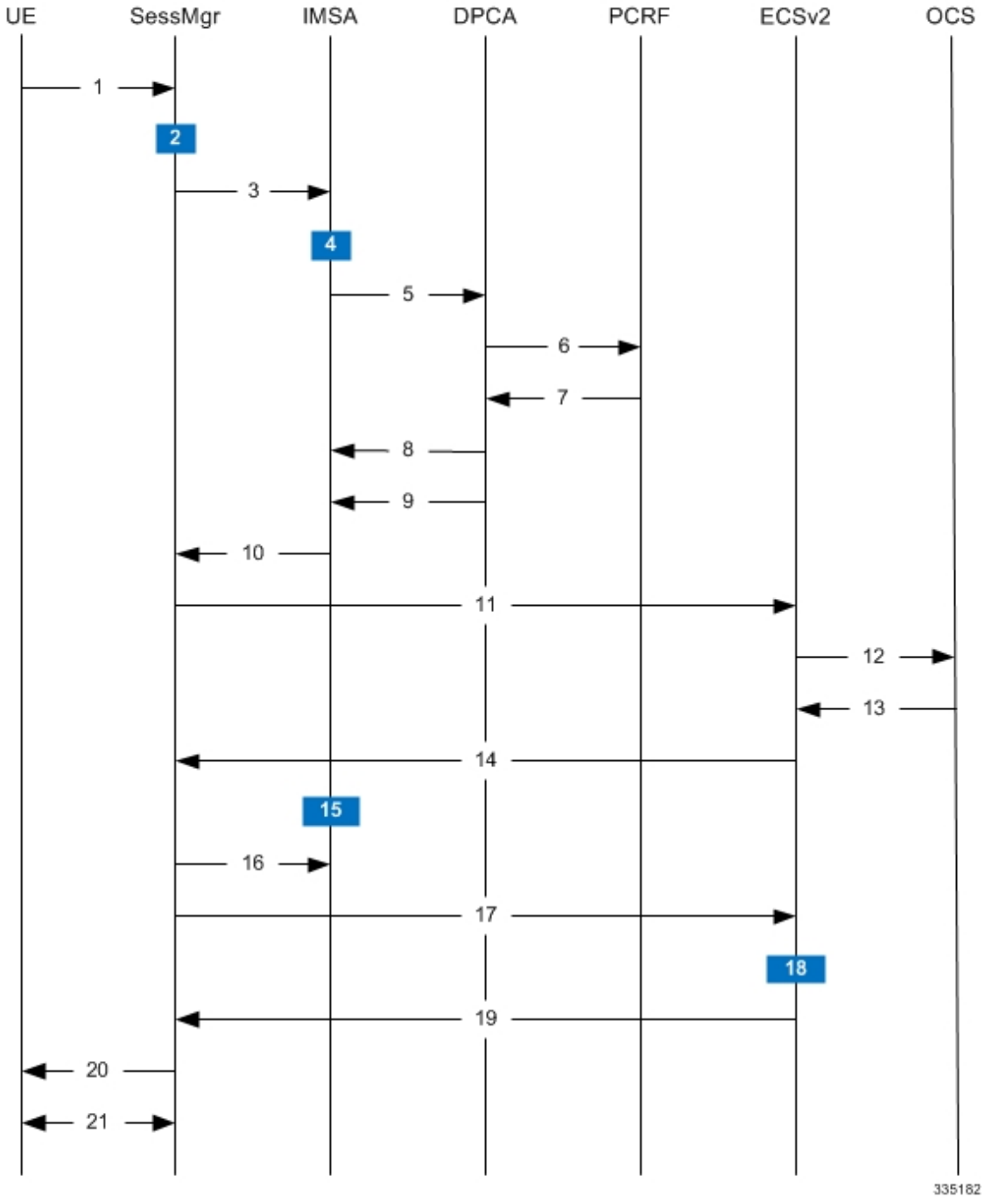


Table 14: Rel. 7 Gx IMS Authorization Call flow Description

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 126.

Step 2 Verify your configuration as described in Verifying the Configuration, on page 128.

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 128.

Step 4 Verify your configuration as described in Verifying Subscriber Configuration, on page 129.

Step 5 *Optional:* Configure the Volume Reporting over Gx feature as described in Configuring Volume Reporting over Gx, on page 129.

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 125.

```
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 15: 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.

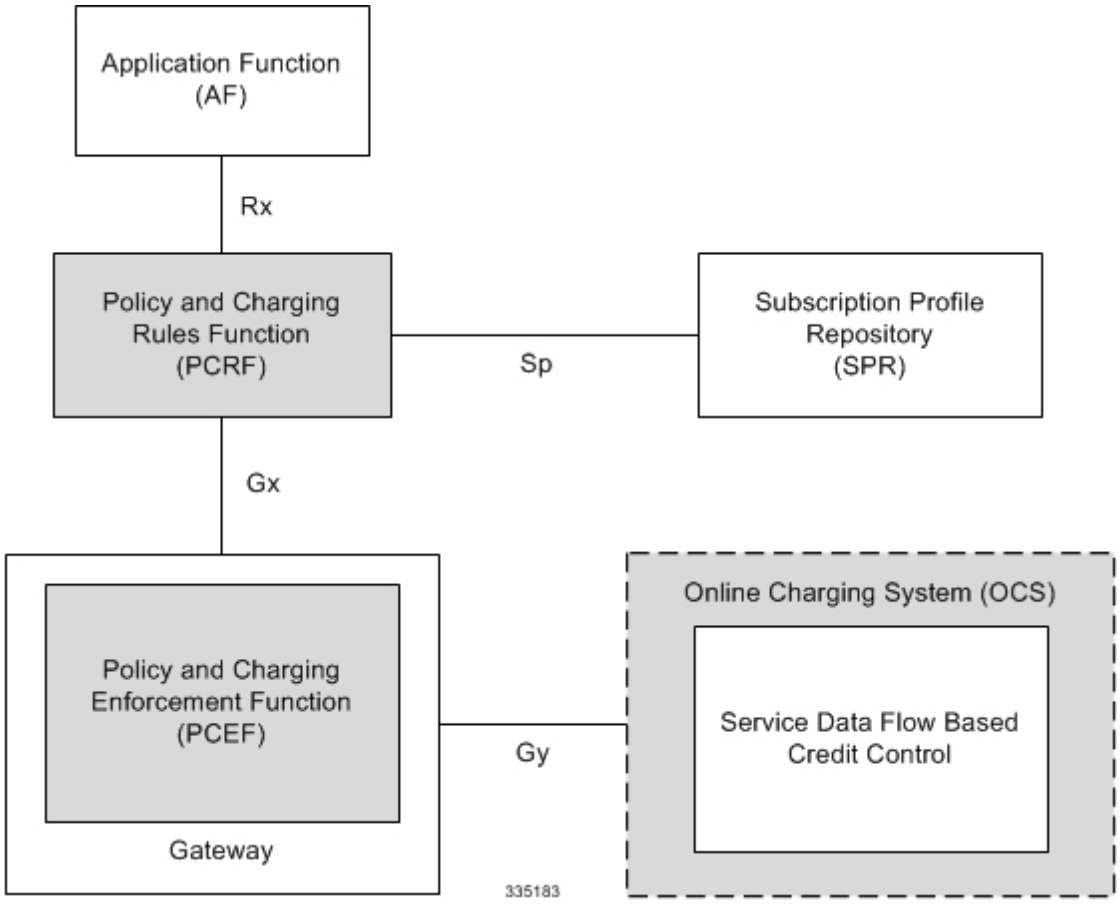
The PCC architecture allows operators to perform service-based QoS policy and FBC control. In the PCC architecture, this is accomplished mainly by the Policy and Charging Enforcement Function (PCEF)/HA/PDSN and the Policy and Charging Rules Function (PCRF). The client functionality lies with the HA/PDSN,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

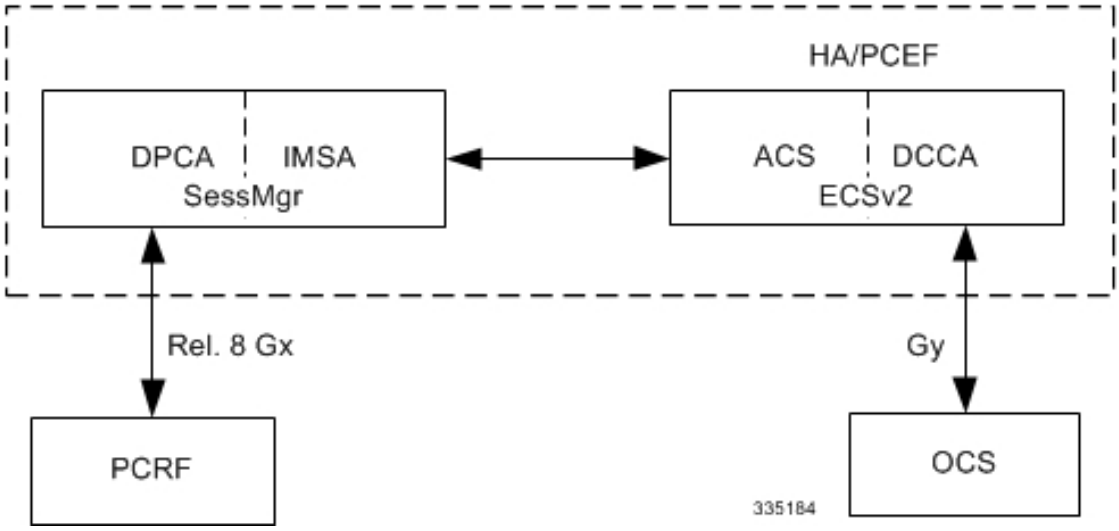
Figure 15: HA/PDSN Rel. 8 Gx PCC Logical Architecture



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 16: 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 17: HA/PDSN Rel. 8 Gx IMS Authorization Call Flow

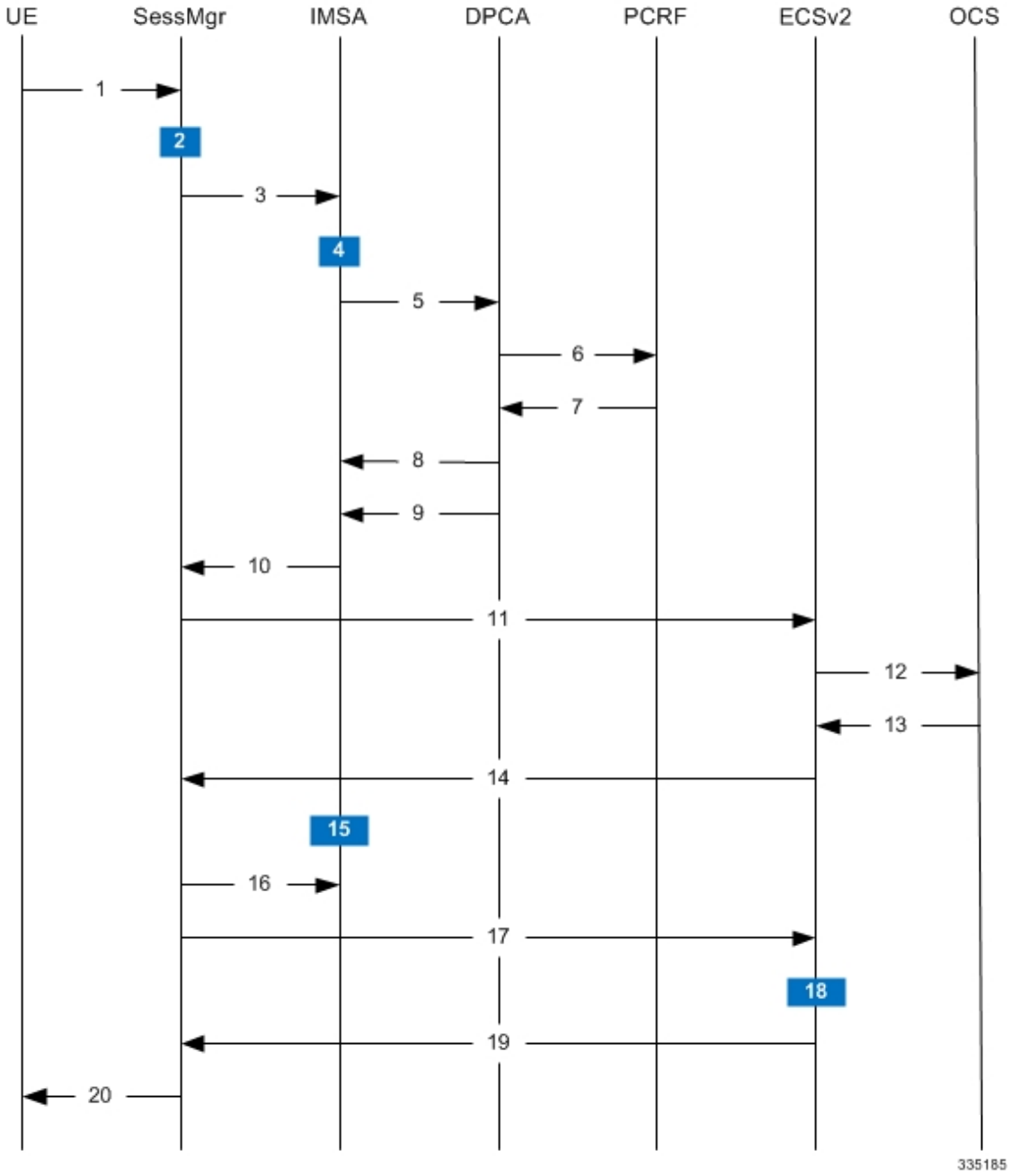


Table 16: HA/PDSN Rel. 8 Gx IMS Authorization Call flow Description

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 145.

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 146.
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 145.

```
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 17: 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 129.

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 129 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 159
- Configuring Rel.9 Compliant AVPs, on page 160
- Monitoring and Troubleshooting the 3GPP Rel.9 Compliance for IPFilterRule, on page 161

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

Gx Interface Support

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 129.

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 174.

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 175.

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 175.

Step 4 Verify your configuration as described in the Verifying Local Policy Service Configuration, on page 175.

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 178.

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.

ADC over Gx Enhancement

With release 21.3.12, the Cisco P-GW is capable of buffering APP_STOP messages for a flow, if the flow matches with a new ADC rule. A maximum of five APP_STOP messages is buffered per flow.

APP_STOP buffering can be enabled with the adc **app-notification** CLI command in the ACS Rulebase Configuration mode. This command should be applied when the flow is being created. Changes to configuration will be applied to the newly created flows.

Important In 21.3.12 and later releases, the **notify** command is deprecated. The **notify** command has been replaced by the command.

When a flow is terminated, all the buffered APP_STOP messages are sent to the PCRF. During flow termination, if the ADC rule is no longer active, the APP_STOP message is not sent to the PCRF.

When a bearer is terminated, the flows present on that bearer are also deleted. On termination, the APP_STOP messages are sent for these flows. APP_STOP messages are only sent for those flows that were present on the bearer at the point of termination.

Since the APP_STOP message is buffered at a flow-level, there is an increase in memory utilization for every rule stored in the Session Manager.

Note This enhancement does not affect the Custom-Mute feature as it is implemented at a flow-level.

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 188
- How it Works, on page 189
- Monitoring and Troubleshooting the TAI and ECGI Change Reporting Feature, on page 190

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
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

Event Trigger from PCRF	CRA Value	Event Detected at P-GW	What to Inform PCRF
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 191

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

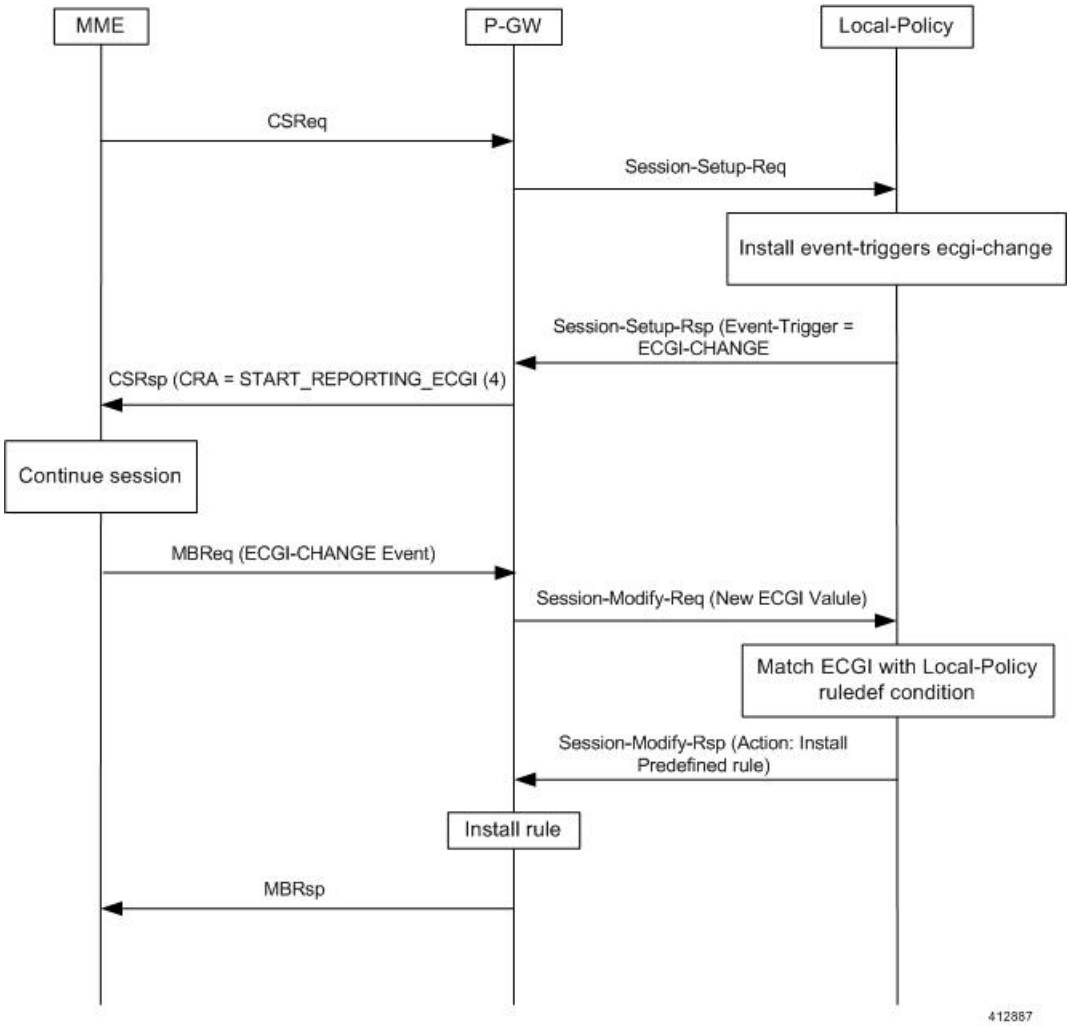
This section describes how the Local Policy Rule selection and enforcement happens based on ECGI-CHANGE event trigger.

Flows

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

Gx Interface Support

Figure 18: 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.

Gx Interface Support

- **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 196
- Configuring Gx based Virtual APN Selection Feature , on page 197
- Monitoring and Troubleshooting the Gx based Virtual APN Selection, on page 197

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:

Gx Interface Support

Table 18: 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.
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.

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 **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.

Gx Interface Support

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 19: 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 20: 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 21: 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, on page 211
- Configuring DPCA for Negotiating Mission Critical QCIs, on page 211
- Monitoring and Troubleshooting the Mission Critical QCI, on page 212

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 22: 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 23: 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

Gx Interface Support

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 24: 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

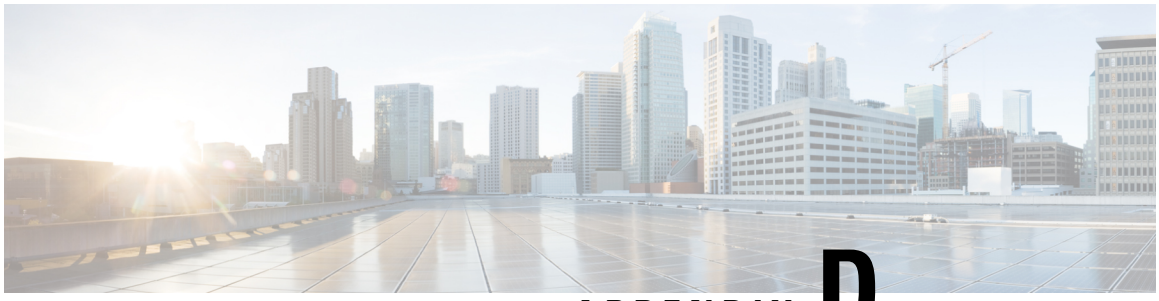
diameter encode-supported-features netloc-ran-nas-cause

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 D

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

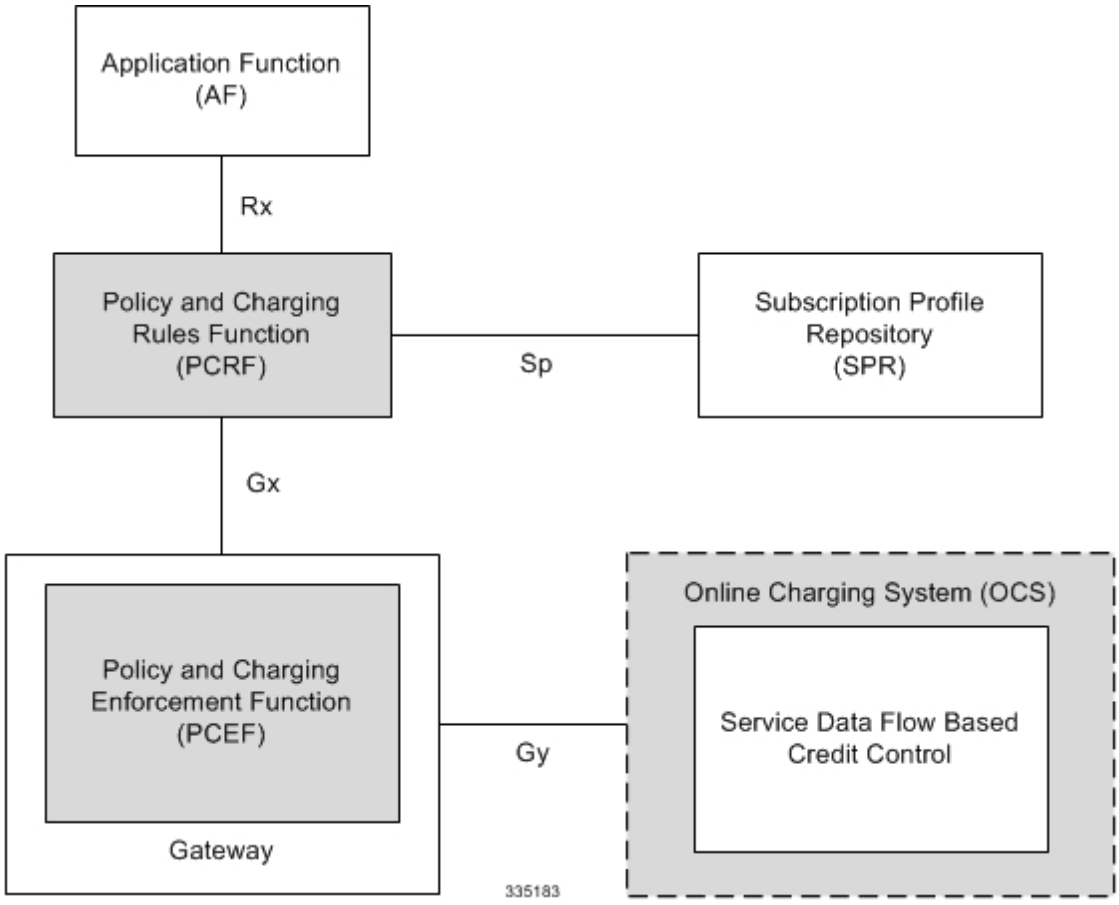
The Gy interface is the online charging interface between the PCEF/GW (Charging Trigger Function (CTF)) and the Online Charging System (Charging-Data-Function (CDF)).

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.

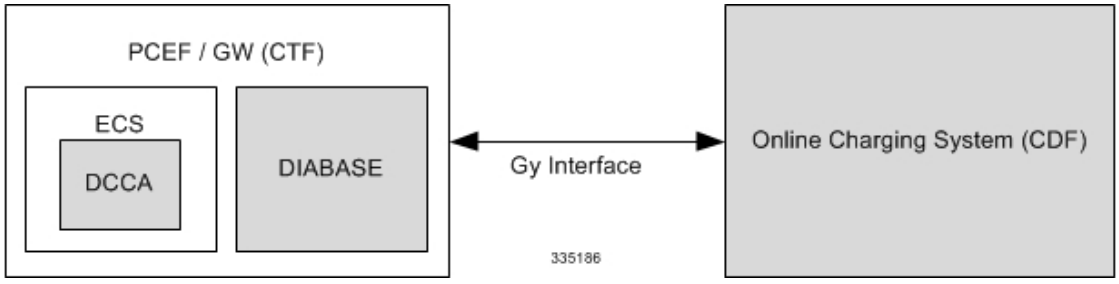
The following figure shows the Gy reference point in the policy and charging architecture.

Figure 19: 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 20: 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)

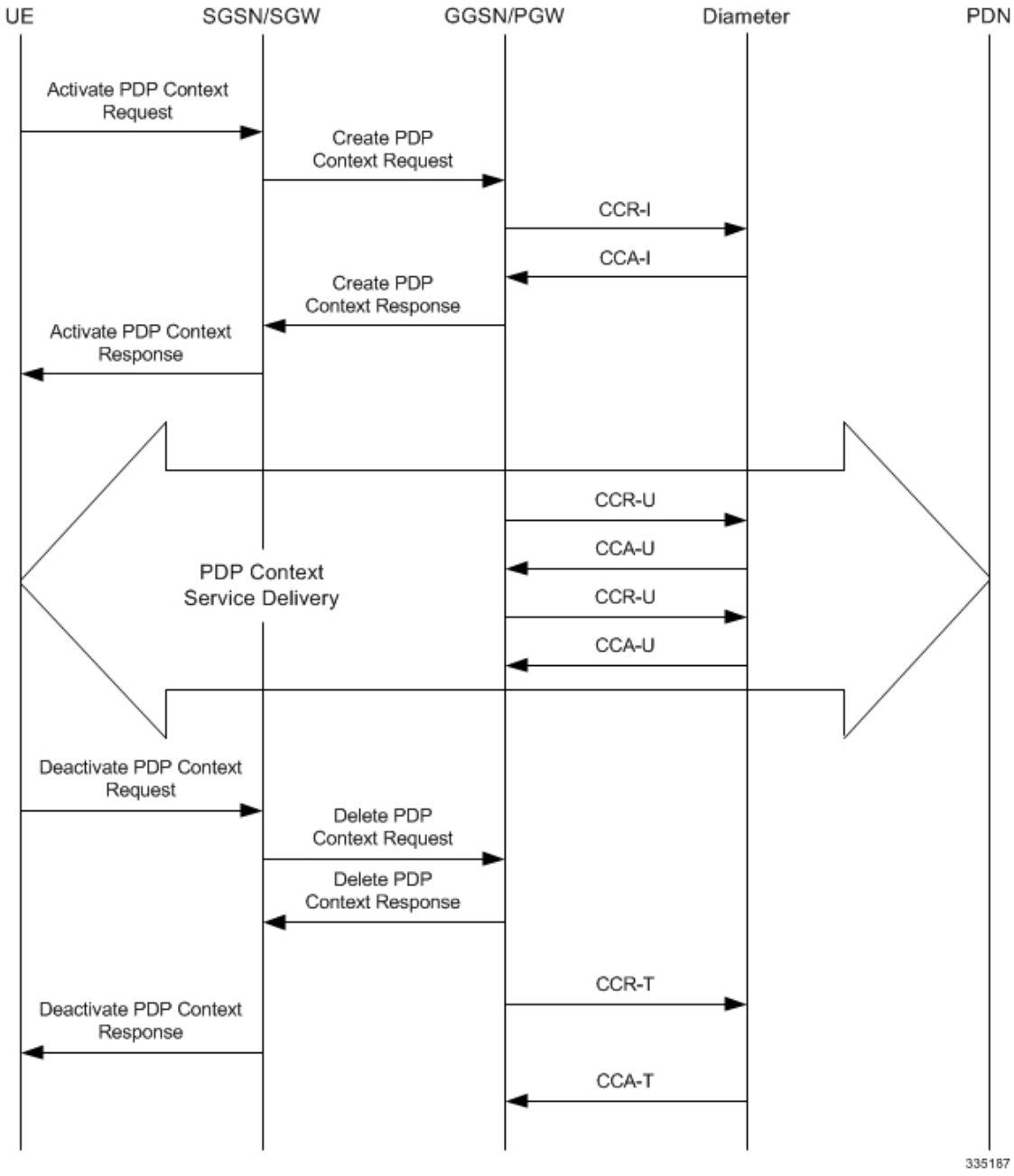
  If the MSCC AVP is missing in CCA-U it is treated as invalid CCA and the session is terminated.
- Credit Control Answer - Terminate (CCA-T)

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.

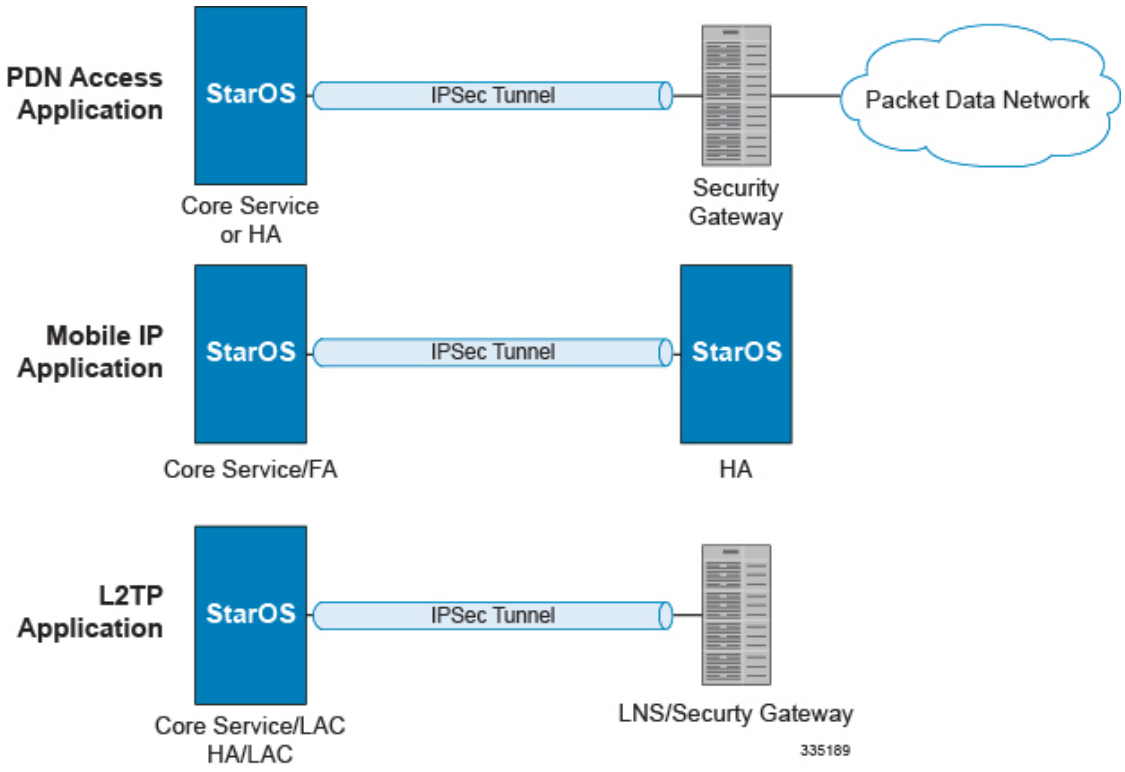
The following figure depicts the call flow for a simple call request in the GGSN/P-GW/IPSG Gy implementation.

Figure 21: 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 22: 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 244.

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)

Gy Interface Support

- Subscription-Id-Type (AVP Code: 450)
- Tariff-Change-Usage (AVP Code: 452):

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

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

  Gy currently supports only IMEISV value.

  Cisco GGSN and P-GW support IMEISV by default.
- User-Equipment-Info-Value (AVP Code: 460)
- Validity-Time (AVP Code: 448)

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

- Offline-Charging (AVP Code: 1278)
- PDP-Address (AVP Code: 1227)
- PDP-Context-Type (AVP Code: 1247)

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

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

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

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

  Only PS-Information is supported.
- SGSN-Address (AVP Code: 1228)
- Time-Quota-Mechanism (AVP Code: 1270):

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

- Supported Diameter AVPs specified in 3GPP TS 32.299 V8.1.0:
  - Auth-Application-Id (AVP Code: 258)
  - Destination-Host (AVP Code: 293)
  - Destination-Realm (AVP Code: 283)
  - Disconnect-Cause (AVP Code: 273)
  - Error-Message (AVP Code: 281)
  - Event-Timestamp (AVP Code: 55)
  - Failed-AVP (AVP Code: 279)

- Multiple-Services-Credit-Control (AVP Code: 456)
- Origin-Host (AVP Code: 264)
- Origin-Realm (AVP Code: 296)
- Origin-State-Id (AVP Code: 278)
- Redirect-Host (AVP Code: 292)
- Redirect-Host-Usage (AVP Code: 261)
- Redirect-Max-Cache-Time (AVP Code: 262)
- Rating-Group (AVP Code: 432)
- Result-Code (AVP Code: 268)
- Route-Record (AVP Code: 282)
- Session-Id (AVP Code: 263)
- Service-Context-Id (AVP Code: 461)
- Service-Identifier (AVP Code: 439)
- Supported-Vendor-Id (AVP Code: 265)
- Termination-Cause (AVP Code: 295)
- Used-Service-Unit (AVP Code: 446)
- User-Name (AVP Code: 1)

Unsupported AVPs

This section lists the AVPs that are NOT supported.

- NOT Supported Credit Control AVPs specified in RFC 4006:
  - CC-Correlation-Id
  - CC-Money
  - CC-Sub-Session-Id
  - CC-Unit-Type (AVP Code: 454)
  - Check-Balance-Result
  - Cost-Information (AVP Code: 423)
  - Cost-Unit (AVP Code: 445)
  - Credit-Control
  - Currency-Code (AVP Code: 425)
  - Direct-Debiting-Failure-Handling (AVP Code: 428)
  - Exponent (AVP Code: 429)

- G-S-U-Pool-Identifier (AVP Code: 453)
- G-S-U-Pool-Reference (AVP Code: 457)
- Requested-Action (AVP Code: 436)
- Service-Parameter-Info (AVP Code: 440)
- Service-Parameter-Type (AVP Code: 441)
- Service-Parameter-Value (AVP Code: 442)
- Unit-Value (AVP Code: 424)
- Value-Digits (AVP Code: 447)

- NOT supported Diameter AVPs specified in 3GPP TS 32.299 V8.1.0:
  - Acct-Application-Id (AVP Code: 259)
  - Error-Reporting-Host (AVP Code: 294)
  - Experimental-Result (AVP Code: 297)
  - Experimental-Result-Code (AVP Code: 298)
  - Proxy-Host
  - Proxy-Info
  - Proxy-State

- NOT supported 3GPP-specific AVPs specified in 3GPP TS 32.299 V8.1.0:
  - 3GPP-CAMEL-Charging-Info (AVP Code: 24)
  - 3GPP-MS-TimeZone (AVP Code: 23)
  - 3GPP-PDSN-MCC-MNC
  - Authorised-QoS
  - Access-Network-Information
  - Adaptations
  - Additional-Content-Information
  - Additional-Type-Information
  - Address-Data
  - Address-Domain
  - Addressee-Type
  - Address-Type
  - AF-Correlation-Information
  - Alternate-Charged-Party-Address
  - Application-provided-Called-Party-Address
  - Application-Server
  - Application-Server-Information
  - Applic-ID
  - Associated-URI
  - Aux-Applic-Info

- Bearer-Service
- Called-Asserted-Identity
- Called-Party-Address
- Calling-Party-Address
- Cause-Code
- Charged-Party
- Class-Identifier
- Content-Class
- Content-Disposition
- Content-Length
- Content-Size
- Content-Type
- Data-Coding-Scheme
- Deferred-Location-Event-Type
- Delivery-Report-Requested
- Destination-Interface
- Domain-Name
- DRM-Content
- Early-Media-Description
- Event
- Event-Type
- Expires
- File-Repair-Supported
- IM-Information
- IMS-Charging-Identifier (ICID)
- IMS-Communication-Service-Identifier
- IMS-Information
- Incoming-Trunk-Group-ID
- Interface-Id
- Interface-Port
- Interface-Text
- Interface-Type
- Inter-Operator-Identifier
- LCS-APN
- LCS-Client-Dialed-By-MS
- LCS-Client-External-ID
- LCS-Client-ID
- LCS-Client-Name
- LCS-Client-Type
- LCS-Data-Coding-Scheme
- LCS-Format-Indicator
- LCS-Information
- LCS-Name-String
- LCS-Requestor-ID
- LCS-Requestor-ID-String
- Location-Estimate

- Location-Estimate-Type
- Location-Type
- Low-Balance-Indication
- MBMS-Information
- MBMS-User-Service-Type
- Media-Initiator-Flag
- Media-Initiator-Party
- Message-Body
- Message-Class
- Message-ID
- Message-Size
- Message-Type
- MMBox-Storage-Requested
- MM-Content-Type
- MMS-Information
- Node-Functionality
- Number-Of-Participants
- Number-Of-Received-Talk-Bursts
- Number-Of-Talk-Bursts
- Originating-IOI
- Originator
- Originator-Address
- Originator-Interface
- Originator-SCCP-Address
- Outgoing-Trunk-Group-ID
- Participant-Access-Priority
- Participants-Group
- Participants-Involved
- PDG-Address
- PDG-Charging-Id
- PoC-Change-Condition
- PoC-Change-Time
- PoC-Controlling-Address
- PoC-Group-Name
- PoC-Information
- PoC-Server-Role
- PoC-Session-Id
- PoC-Session-Initialtion-Type
- PoC-Session-Type
- PoC-User-Role
- PoC-User-Role-IDs
- PoC-User-Role-info-Units
- Positioning-Data
- Priority
- PS-Append-Free-Format-Data (AVP Code: 867):

The PCEF/GW ignores this AVP if no PS free format data is stored for the online charging session.

- PS-Free-Format-Data (AVP Code: 866)
- PS-Furnish-Charging-Information (AVP Code: 865)
- RAI (AVP Code: 909)
- Read-Reply-Report-Requested
- Received-Talk-Burst-Time
- Received-Talk-Burst-Volume
- Recipient-Address
- Recipient-SCCP-Address
- Refund-Information
- Remaining-Balance
- Reply-Applic-ID
- Reply-Path-Requested
- Requested-Party-Address
- Role-of-node
- SDP-Answer-Timestamp
- SDP-Media-Component
- SDP-Media-Description
- SDP-Media-Name
- SDP-Offer-Timestamp
- SDP-Session-Description
- SDP-TimeStamp
- Served-Party-IP-Address
- Service-Generic-Information
- Service-ID
- Service-Specific-Data
- Service-Specific-Info
- Service-Specific-Type
- SIP-Method
- SIP-Request-Timestamp
- SIP-Response-Timestamp
- SM-Discharge-Time
- SM-Message-Type
- SM-Protocol-Id
- SMSC-Address
- SMS-Information
- SMS-Node
- SM-Status
- SM-User-Data-Header
- Submission-Time
- Talk-Burst-Exchange
- Talk-Burst-Time
- Talk-Burst-Volume
- Terminating-IOI

- Time-Stamps
- Token-Text
- Trunk-Group-ID
- Type-Number
- User-Participating-Type
- User-Session-ID
- WAG-Address
- WAG-PLMN-Id
- WLAN-Information
- WLAN-Radio-Container
- WLAN-Session-Id
- WLAN-Technology
- WLAN-UE-Local-IPAddress

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.

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, on page 264
- Configuring Credit-Control Group in Rulebase, on page 265
- Monitoring and Troubleshooting the CC-Group Selection in Rulebase, on page 266

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
```

Important After you configure these 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.

- *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 271 and Configuring HA / PDSN Gy Interface Support, on page 272.

Step 3 Configure Event-based Gy support as described in Configuring PLMN and Time Zone Reporting, on page 273.

Step 4 *Optional.* Configure OCS Unreachable Failure Handling Feature or Assume Positive for Gy Feature as described in Configuring Server Unreachable Feature, on page 274.

Step 5 *Optional.* Configure Static Rulebase for CCR as described in Configuring Static Rulebase for CCR, on page 275.

Step 6 *Optional.* Configure Gy for GTP based S2a/S2b as described in Configuring Gy for GTP based S2a/S2b, on page 275.

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.

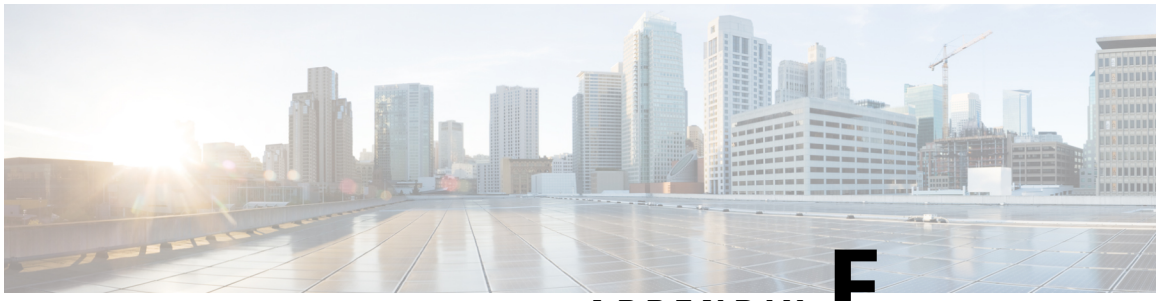
Important After you configure **configure**, **require active-charging**, **active-charging service** *service_name*, and **credit-control group** *ccgroup_name* CLI commands, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration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

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**
States of the Credit Control application's sessions, DCCA.	**show active-charging credit-control session-states [rulebase** <*rulebase_name*> **] [content-id** <*content_id*> **]**



APPENDIX E

HA Redundancy for Dynamic Home Agent Assignment

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 before using the procedures in this chapter.

This chapter includes the following topics:

Feature Description

This feature provides a mechanism for a system functioning as a Home Agent (HA) to communicate status information to a properly configured RADIUS server. The status information is used by the RADIUS server to determine the availability and readiness of the HA to accept Mobile IP (MIP) subscriber sessions. The RADIUS server\'s awareness of the HA status allows it to dynamically assign immediately available HAs to subscriber sessions.

When a RADIUS server assigns an HA to a Mobile Node (MN), it is very important that only active, or accessible, HAs are selected for the assignment. Therefore, it is necessary for the RADIUS server to detect the availability of each HA before assigning it to an MN. This feature allows the RADIUS server to gather and maintain a list of available HAs through a detection mechanism that provides frequent updates.

With this feature, bogus authentication messages, called probe authentication messages, are exchanged between the RADIUS server and the HA. The HA periodically sends Access-Request messages to the RADIUS server. The RADIUS server distinguishes the probe authentication request from other regular subscriber authentication messages, validates them, and sends proper response.

The probe Access-Request contains the following attributes and expects an Access-Accept from the RADIUS server.

```
User-Name = Probe-User
User-Password = 18 7F 88 02 82 1D B6 F6 70 48 B9 A1 4C 92 C3 3E
NAS-IP-Address = 182.168.65.2
Service-Type = Authenticate_Only
Event-Timestamp = 1255598429
```

User-Name and User-Password are configurable in the system.

If an Access-Accept message is sent in response to the probe authentication request, the RADIUS server updates the status of the HA as active. If an Access-Reject message is sent, the RADIUS server updates only the statistics without any further action. If the RADIUS server misses receiving a configured number of probe authentication requests, the HA, and all of its associated IP addresses, is marked as down, or inaccessible. When an HA is marked as down, a backup HA and its associated IP addresses are made active and used for assignment in the place of the inaccessible HA.

Supported Implementations

This feature is supported on system installations that are configured as Home Agents and are configured to communicate with a AAA Service Controller that supports the configuration of Active and Backup HAs. For more information on a compatible AAA Service Controller, contact your designated customer support engineer.

Configuring HA Redundancy for Dynamic Home Agent Assignment

Before you begin

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

Step 1 Configure the AAA Service Controller as described in the AAA Service Controller documentation.

Step 2 Configure RADIUS support on the HA as described in the Configuring RADIUS Support on the HA, on page 279 section.

Step 3 Save the 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*.

What to do next

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 the AAA Service Controller

The AAA Service Controller should be configured with the following parameters. For configuration information refer to the AAA Service Controller documentation.

- Authentication-Probe User profile:

    - Probe Username
    - Probe Password
- HA Client information:
    - HA Client IPv4 address (NAS-IP-Address attribute)
    - HA client secret (authenticator)
    - Whether the HA client is a Primary or Backup HA client
- One or more HA Service addresses for each HA client address.
- The number of missed probe authentication requests before the HA Client is marked as down.
- The number of seconds to wait for a probe authentication request from the HA client (timeout period).
- The number of seconds to wait for a backup HA server to be in the active state after a reboot, known as backup-hold-timeout.

Configuring RADIUS Support on the HA

Use the following example to configure RADIUS support on the HA:

```
configure
 context <context_name>
 radius server <ip_address> [ encrypted ] key <value>
 radius probe-interval <seconds>
 radius probe-max-retries <retries>
 radius probe-timeout <idle_seconds>
 end
```

Notes:

- <context_name> must be the name of the AAA context that the HA service uses for authentication.
- A number of optional keywords and variables are available for the **radius server** command. Refer to the *Command Line Interface Reference* for more information regarding this command.
- Option: To configure HA redundancy with AAA server group, in the Context Configuration Mode, use the following command:

  aaa group <*group_name*>

  <*group_name*> must be the name of the AAA group designated for AAA functionality within the context. A total of 400 server groups can be configured system-wide including the default server-group unless **aaa large-configuration** is enabled. For information on configuring context-level AAA functionality, refer to the AAA Interface Administration and Reference.

Important After you configure the **aaa large-configuration** 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.

Verifying RADIUS Server Configurations

This section provides information to verify connectivity to the RADIUS server, and information to view counters and statistics that can be useful in troubleshooting issues.

Step 1 Verify connectivity to the RADIUS server by sending a test probe message to the RADIUS server by entering the following command:

radius test probe authentication server <*ip_address*> **port** <*port_number*> [**username** <*username*> **password** <*password*>]

Important Any response, including **Access-Reject** and **Access-Accept** from the AAA server, is considered to mean that the AAA server is alive.

The following is a sample of the output of a successful probe authentication test.

```
[local]host_name radius test probe authentication server 192.168.20.1 port 1812
Authentication from authentication server 192.168.20.1, port 1812
Authentication Success: Access-Accept received
Round-trip time for response was 714.2 ms
```

Step 2 View the RADIUS counters by entering the following command:

show radius counters { all | server <*ip_address*> [**port** <*port_number*>] } [| { **grep** <*grep_options*> | **more** }]

The following is a sample output of the command displaying RADIUS Probe counters.

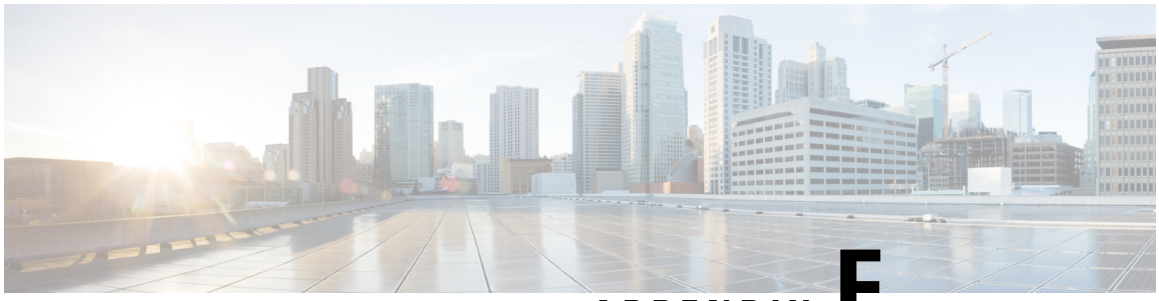
```
Server-specific Probing Counters
   --------------------------------
     State: Down
     Number of transactions issued:3
     Number of successful transactions:2
     Number of failed transactions:1
     Last successful transaction time: Thu Aug 26 17:40:32 2004
     Last failed transaction time:Thu Aug 26 17:40:39 2004
     Last roundtrip time:3.2 ms
```

Step 3 View AAA Manager statistics by entering the following command:

show session subsystem [full | facility *aaamgr* [**all | instance** <*id*>]] [**verbose**] [| { **grep** <*grep_options*> | **more** }]

The following is a sample output of the command displaying authentication probe statistics in the output.

```
AAAMgr:  Instance 261
       4 Total aaa requests                  0 Current aaa requests
       3 Total aaa auth requests             0 Current aaa auth requests
       0 Total aaa auth probes               0 Current aaa auth probes
       1 Total aaa acct requests             0 Current aaa acct requests
```



APPENDIX F

Network Mobility (NEMO)

This chapter describes the system\'s support for Network Mobility (NEMO) and explains how it is configured. 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 the respective product Administration Guide, before using the procedures in this chapter.

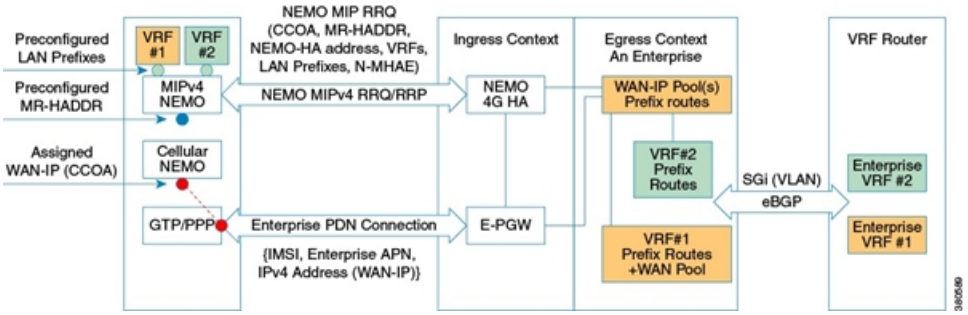
NEMO Overview

When enabled through a feature license key, the system includes NEMO support for a Mobile IPv4 Network Mobility (NEMO-HA) on the existing Enterprise Home Agent (EHA) platform to interconnect LAN segments behind Mobile Routers (MRs) equipped with a 3G interface with Fixed Networks served by the Private IP (PIP) networks and Wavelength Division Multiplexing Networks (WDN) . The new NEMO functionality allows bi-directional communication that is application-agnostic between users behind the MR and users or resources on the Fixed Network sites.

The same NEMO4G-HA service and its bound Loopback IP address supports NEMO connections whose underlying PDN connection comes through GTP S5 (4G access) or PMIPv6 S2a (eHRPD access).

The following figure shows a high-level view of NEMOv4 Architecture.

Figure 23: NEMO Overview



Features and Benefits

The system supports the usage of dynamically learned, overlapping customer prefixes. These prefixes are advertised through BGP in a manner similar to pool routes in the current EHA implementation. NEMO includes the following features:

- Interoperates with the Mobile IPv4 NEMO implementation of the Cisco ISR CPE routers.
  - Protocol behavior.
  - Message structures, formats and encoding.
  - Specific flags and parameters.
- Compatible with the specifics of the Mobile IPv4 NEMO operation of the Cisco ISR CPE routers.
  - Support for the second Mobile IPv4 NEMO Control Messaging.
  - Support for GRE NEMO-Tunnel termination (One NEMO-Tunnel per MR).
  - Support for explicit LAN Prefix registration mode.
- Support for private customer addressing, routing and traffic segmentation
  - Private and overlapping WAN-IP addresses.
  - Private and overlapping LAN Prefixes.
  - Customer LAN Prefix advertisement from the EHA egress contexts via BGP
  - Customer traffic segmentation and mapping of the incoming NEMO-Tunnels to the appropriate VLAN/VRF.
- Ability to seamlessly integrate with the existing MPN service environment.
  - Selective suppression or replacement of specific fields in the NEMO Mobile IPv4 Control Messaging sourced by the CPE routers.
  - Correlation of the incoming NEMO Control and Forwarding traffic with the existing control and flow structures related to the HWIC device processing by the underlying IS-835/MIP logic in the EHA.
  - Compatibility with the existing AAA requirements.
- The HWIC IS-835/PPP/MIP timers shall be compatible with today's EHA implementation.
  - PDSN's PPP idle timeout (2 hrs)
  - PDSN's PPP absolute timer (24 hrs)
  - First MIP session re-registration timer (1hr 55min)

- NEMO-HA is not required to generate AAA accounting records (START/STOP) for the NEMO MIP session. On the other hand, accounting records are generated for the MR's HWIC MIP session, just like with any other MIP sessions.
- NEMO-HA supports explicit registration mode and does not require authorization/validation of the LAN Prefixes sent by the MR.
- If the authentication of the NEMO MIP session fails, the underlying HWIC IS-835/MIP session is maintained since the NEMO function may attempt to establish the NEMO-Tunnel again.
- NEMO-HA is supported by ICSR. All the information related to NEMO-HA (NEMO MIP session state, and so on) is synchronized with the standby EHA and the total failure of the active EHA does not require existing NEMO tunnels to be re-established.
- NEMO-HA has dynamically advertise the LAN prefixes of any given MR to the upstream corporate router, but it does have the ability to suppress the MR's MR-HADDR address from the route advertisement via route-map configuration.
- The existing EHA support for interface MTU configuration also applies to NEMO-HA enabled systems.
- The NEMO-HA supports Local Authentication - the N-MHAE-SPI/KEY values are stored in the NEMO-HA. NEMO-HA supports two options to provision the SPI/KEY information in the MR's:
  - Individual MR level: each MR would has a unique SPI/KEY pair.
  - Enterprise level: each Enterprise uses unique security credentials and all the MR's of a given Enterprise uses the same SPI/KEY pair.
- A new RADIUS attribute (VSA) is supported that can be passed to the EHA during the establishment of the first IS-835/MIP session between the MR's HWIC and the EHA. This new RADIUS attribute represents the authorization of a second NEMO MIP RRQ for the associated MR. The EHA verifies if the new NEMO-related VSA is present in the Access-Accept for the first IS-835/MIP session. If so, NEMO-HA caches this information to properly authorize the second NEMO MIP session. This allows the AAA to control the authorization of NEMO sessions more efficiently without the need for a second AAA message.
- Upon any failure with the establishment of a second NEMO MIP session, the EHA does not take any actions with the underlying IS-835/MIP session. In other words, it does not tear down the first IS-835/MIP session.
- The NEMO-HA supports overlapping WAN-IP addresses for differing enterprises.
- RFC 5177 is supported.
- Enterprise VLANs are unique to the enterprise. Two different enterprises do not share the same VLAN ID in the egress context(s)
- If no NEMO-HA service is defined, it is not using NEMO.
- The NEMO HA support both dynamic address allocation and static address assignment.
- Multi-VRF - The existing design of HA NEMOv4 is extended to allow more than one VRF. For more information on Multi VRF, see *NEMOv4 with Multi-VRFs*.
- Enterprise minimal-registration-lifetime overwrite.
- PMIPv6 - Mobile Private Network (MPN) utilized Network Mobility Services (NEMO) to provide wireless connectivity between Enterprise Core Network and remote Enterprise sites over 3G/4G network, and supported only IPv4 addressing scheme. To expand the addressing scheme to IPv6, PMIPv6 support is now added. The LMA functionality will be provided externally by the ASR9000.

Engineering Rules

- Up to 300 virtual routing tables per context and 64 BGP peers per context.

- Up to 5k host routes spread across multiple VRFs per BGP process. Limited to 6000 pool routes per chassis.
- Up to 2048 VRFs per chassis.
- Up to 512K NEMO framed MNPs (Mobile Private Networks) per system.
- 32K routes per context.

Supported Standards

- IETF RFC 5177 (April 2008) "Mobile IPv4 NEMO Extensions,"
- IETF RFC 3025 (February 2001) "Mobile IP Vendor/Organization Specific Extensions"

NEMO Configuration

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

To configure the system for NEMO:

1. Create a VRF on the router and assign a VRF name.
2. Set the neighbors and address family to exchange routing information with a peer router.
3. Redistribute connected routes between routing domains.
4. Create a NEMO HA.
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*.

Sample Configuration

```
config ingress
    context ingress
      interface <interface-name> loopback
          ip address <ipaddress> srp-activate
      exit
      interface <interface-name> loopback
          ip address <ipaddress> srp-activate
      exit
      interface <interface-name> loopback
          ip address <ipaddress>
      exit
      subscriber name <subscriber-name>
          encrypted password +A0ma96jknt7xul1ne8fk1kuled82o27x1i1fw6t103rqedigdfacp
          ip context-name egress1
            ip address pool name <pool-name>
```

```
          permission nemo
      exit
      ha-service <ha-service-name>
          mn-ha-spi spi-number <256>  encrypted secret
+A2ityhei4lza673nh1o9nqr4yqm2gsp0yv8eflng2tn2cyh5t1fbn hash-algorithm md5
          authentication mn-aaa noauth
            authentication mn-ha allow-noauth
          encapsulation allow keyless-gre
          min-reg-lifetime <300>
         bind address +A2ityhei4lza673nh1o9nqr4yqm2gsp0yv8eflng2tn2cyh5t1fbn hash-algorithm
 md5
      exit
      ha-service enterprise-ha1
          mn-ha-spi spi-number <256>  encrypted secret
+A0zsddshr3maez0b9j3izuk6q5612m1itttjmwyg16hiussxb5byv hash-algorithm md5 timestamp-tolerance
 65535
          fa-ha-spi remote-address ipaddress spi-number <256> encrypted secret
+A2yxbf7x14k8ko2aeef6fxrklft2zmir909mdp1n26ppovmlnw41w hash-algorithm md5 timestamp-tolerance
 65535
          authentication mn-ha allow-noauth
          revocation enable
          reg-lifetime <7200>
          bind address <ipaddress>
      exit
      ha-service <enterprise-ha2>
          mn-ha-spi spi-number <256>  encrypted secret
+A0zsddshr3maez0b9j3izuk6q5612m1itttjmwyg16hiussxb5byv hash-algorithm md5 timestamp-tolerance
 65535
          fa-ha-spi remote-address ipaddress spi-number <256> encrypted secret
+A2yxbf7x14k8ko2aeef6fxrklft2zmir909mdp1n26ppovmlnw41w hash-algorithm md5 timestamp-tolerance
 65535
            authentication mn-ha allow-noauth
          revocation enable
          reg-lifetime 7200
          bind address <ipaddress>
      exit
end
```

Ingress with new ComboHA feature.

Important Everything is same for NEMO except changes for IS-835/MIP session.

```
config
      interface <interface-name> loopback
          ip ranged-address ipaddress srp-activate
      exit
      ha-service <ha-service-name>
          mn-ha-spi spi-number <256>  encrypted secret
+A1ere1vystx2r7056dq8i1o5h3m1e0xpcwghhhe80e3q3251jggkf hash-algorithm md5 timestamp-tolerance
 65535
          fa-ha-spi remote-address ipaddress spi-number <256> encrypted secret
+A2xya6hjckox7c2964eftaufx1530khglavl7urf0nknletmp5dro hash-algorithm md5 timestamp-tolerance
 65535
          fa-ha-spi remote-address ipaddress spi-number <256> encrypted secret
+A1nexk5t8kjbav0vd7thh0yv4ly1ms68mtcermok0mxx2brve2ot7 hash-algorithm md5 timestamp-tolerance
 65535
          authentication mn-ha allow-noauth
          revocation enable
          reg-lifetime 7200
```

```
        bind address <ipaddress>
    exit
end
```

NEMO Egress

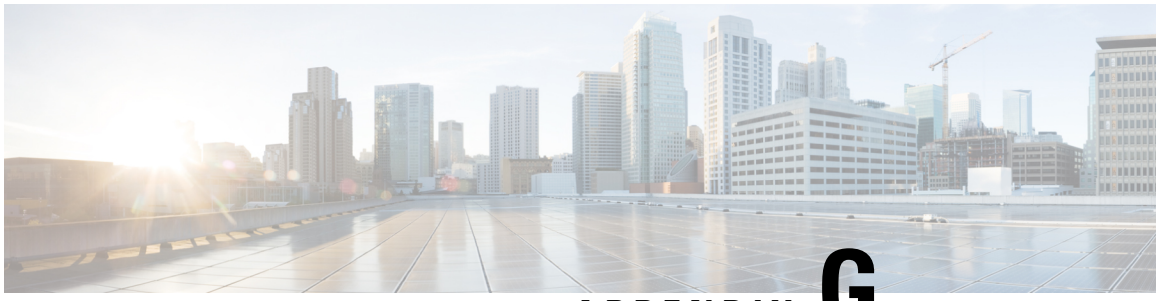
```
config
  context egress1
    ip vrf <vrf-name1>
        ip maximum-routes 4998
    exit
    ip vrf <vrf-name2>
        ip maximum-routes 4998
    exit
    ip vrf <vrf-name3>
        ip maximum-routes 4998
    exit
    ip routing overlap-pool
    ip pool cust1-f <ipaddress> private 0 group-name customer1 vrf <vrf-name1>
nexthop-forwarding-address ipaddress overlap vlanid 401 policy allow-static-allocation
    ip pool cust2-f ipaddress private 0 group-name customer2 vrf <vrf-name2>
nexthop-forwarding-address ipaddress overlap vlanid 402 policy allow-static-allocation
    ip pool <pool-name> ipaddress private 0 group-name customer3 vrf
<vrf-name3>nexthop-forwarding-address <ipaddress>overlap vlanid 403 policy
allow-static-allocation
    router bgp 1
        enforce-first-as
        neighbor <ipaddress> remote-as <1001>
        neighbor <ipaddress> update-source <ipaddress>
        neighbor <ipaddress> remote-as <1001>
        neighbor <ipaddress> update-source <ipaddress>
        ip vrf <vrf-name1>
            route-distinguisher 1 1
        exit
        address-family ipv4 vrf  <vrf-name1>
            redistribute connected
            neighbor <ipaddress> remote-as 1001
            neighbor <ipaddress> use-default-table
            neighbor <ipaddress> ebgp-multihop max-hop 255
            neighbor <ipaddress> update-source ipaddress
            neighbor <ipaddress> remote-as 1001
            neighbor <ipaddress> use-default-table
            neighbor <ipaddress> ebgp-multihop max-hop 255
            neighbor <ipaddress> update-source <ipaddress>
        exit
        ip vrf vrf-cust2
            route-distinguisher 1 2
        exit
            address-family ipv4 vrf <vrf-name2>
            redistribute connected
            neighbor ipaddress remote-as 1001
            neighbor ipaddress use-default-table
            neighbor ipaddress ebgp-multihop max-hop 255
            neighbor ipaddress update-source ipaddress
            neighbor ipaddress remote-as 1001
            neighbor ipaddress use-default-table
            neighbor ipaddress ebgp-multihop max-hop 255
            neighbor ipaddress update-source ipaddress
        exit
        ip vrf <vrf-name2>
            route-distinguisher 1 3
        exit
        address-family ipv4 vrf  <vrf-name3>
```

```
            redistribute connected
            neighbor <ipaddress> remote-as 1001
            neighbor <ipaddress> use-default-table
            neighbor <ipaddress> ebgp-multihop max-hop 255
            neighbor <ipaddress> update-source <ipaddress>
            neighbor <ipaddress> remote-as 1001
            neighbor <ipaddress> use-default-table
            neighbor <ipaddress> ebgp-multihop max-hop 255
            neighbor <ipaddress> update-source <ipaddress>
        exit
        interface 29/1-sub401
            ip address ipaddress
        exit
        interface 29/1-sub402
            ip address <ipaddress>
        exit
        interface 29/1-sub403
            ip address <ipaddress>
    exit
end
```

NEMO MPLS Egress

```
config
context egress1
    ip vrf<vrf-cust1>
        ip maximum-routes 4998
    exit
    ip vrf <vrf-cust2>
        ip maximum-routes 4998
    exit
    ip vrf <vrf-cust3>
        ip maximum-routes 4998
    exit
    mpls bgp forwarding
    ip pool pool1-b <ipaddress> private 0 srp-activate group-name customer1 vrf vrf1
policy allow-static-allocation
    ip pool pool2-b <ipaddress> private 0 srp-activate group-name customer2 vrf vrf2
policy allow-static-allocation
    ip pool pool3-b <ipaddress> private 0 srp-activate group-name customer3 vrf vrf3
policy allow-static-allocation
    router bgp 1
        router-id ipaddress
        neighbor <ipaddress> remote-as 1001
        neighbor <ipaddress> remote-as 1001
        timers bgp keepalive-interval 10 holdtime-interval 30
        address-family vpnv4
            neighbor <ipaddress> activate
            neighbor <ipaddress> send-community both
            neighbor <ipaddress> activate
            neighbor <ipaddress> send-community both
        exit
        ip vrf <vrf1>
            route-distinguisher 1 1
            route-target export 1 1
            route-target import 1 1
        exit
        address-family ipv4 vrf <vrf1>
            redistribute connected
            redistribute static
        exit
        ip vrf <vrf2>
            route-distinguisher 2 2
```

```
            route-target export 2 2
            route-target import 2 2
        exit
        address-family ipv4 vrf <vrf2>
            redistribute connected
            redistribute static
        exit
        ip vrf <vrf3>
            route-distinguisher 3 3
            route-target export 3 3
            route-target import 3 3
        exit
        address-family ipv4 vrf <vrf3>
            redistribute connected
            redistribute static
        exit
end
```



APPENDIX G

NEMOv4 with Multi-VRFs

This chapter describes the system's support for Network Mobility V4 (NEMOv4) with Multi-VRFs and explains how it is configured. 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 the respective product Administration Guide, before using the procedures in this chapter.

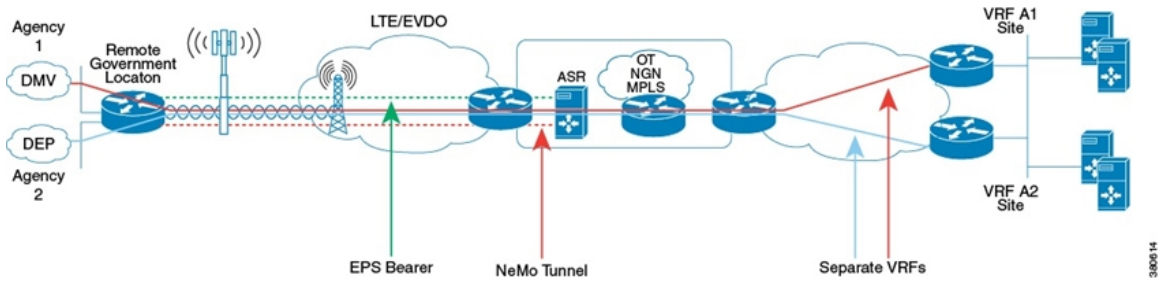
NEMO Overview

The existing design of HA NEMOv4 has been extended to support multiple enterprise network being connected from one Mobile Router. A Mobile Router (MR) can be configured with devices/subnets to seamlessly access multiple enterprize VRFs, and the network traffic targeted for those different VRFs will share same MIP tunnel without compromising the privacy and security. Each VRF works independently through the MR and HA services.

This is done by separating the VRFs at the NEMO registration time, each VRF will be furnished with own set of GRE keys for the bidirectional traffic between MR and HA.

The following figure shows a high-level view of Multi-VRF Support.

Figure 24: Multi-VRF-Support



Use Cases

The following use cases are supported by NEMO Multi-VRF. Multi-VRF provides a simplified CPE/UE configuration, strong privacy and separation between networks, without impacting an organization's IP addressing or routing designs or protocols. :

1. **Multi-Agency:** A Remote Government location that supports multiple agencies which require overlapping IP addresses and privacy.
2. **Multi-Tenant:** Multiple customers using a single mobile router/access line, across any network, with special affinity for LTE, allowing the service provider to provide multi-tenant services at a location. For example, multi-tenant buildings, fast food restaurants with multiple companies.
3. **Machine-to-Machine (M2M):** Allows multiple services or machines to share a mobile router or access line within a single Kiosk/ATM/multi-function device. For exmaple, ATM, retail kiosk, vending machines, automobiles, trucks, trains, planes, mobile setups/shows.
4. **Guest Access:** Allows corporate access and guest/Internet access to share a mobile router/access line, or to share a mobile router. For example, Retail store, restaurant, entertainment venue, planes, trains, cars (separate from car functions), Teleworker/Home.
5. **SMB/Residential Gateway:** Allows multiple SMB office or residential services/devices to share a mobile router/access line within a single residential home router. For example, Homes, Teleworker, doctor offices, real estate offices, small businesses, temporary sites.

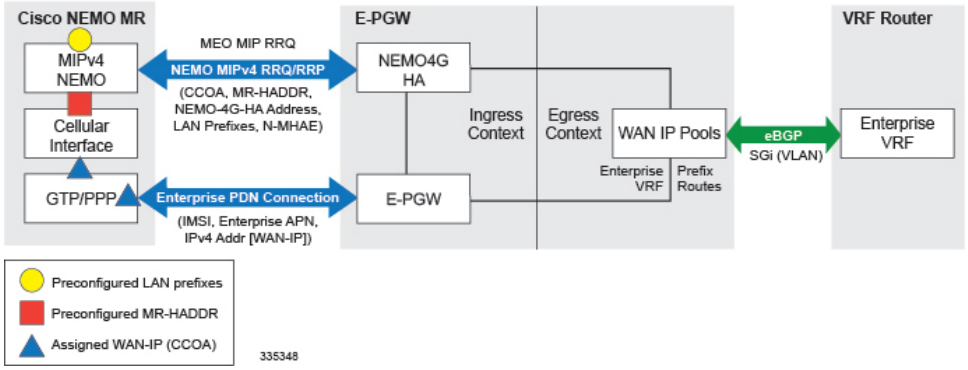
Features and Benefits

The system supports the usage of dynamically learned, overlapping customer prefixes. These prefixes are advertised via BGP.

MIPv4-based NEMO Control Plane

The following figure shows a high-level view of the NEMO control plane.

Figure 25: NEMO Control Plane



NEMO includes the following features:

- Collocated-Care-of-Address mode

  The Cisco NEMO MR is expected to use the Collocated-Care-of-Address mode to establish a NEMO MIPv4 session with NEMO4G-HA and as one of the IP endpoints of the NEMO GRE Tunnel for the transport of user traffic.

- MR-HADDR

  NEMO4G-HA supports a potential "dummy" MR-HADDR address that would be configured in every MR within the same Enterprise or across all served Enterprises (same IP address). NEMO4G-HA supports the registration for Mobile Router services.

- Dynamic advertisement of WAN-IP Pools and learned LAN prefixes

  eBGP is used to advertise the Enterprise WAN-IP Pools and the LAN prefixes learned via NEMO for the associated Enterprise.

- N-MHAE credentials

  NEMO4G-HA supports local authentication for the NEMO MIPv4 RRQ based on preconfigured N-MHAE-SPI/KEY values on a per Enterprise basis (one unique set for all MRs belonging to the same Enterprise) or on a global basis (one unique set for all Enterprises).

- LAN prefixes
  - NEMO4G-HA accepts a minimum of zero LAN prefixes and a maximum of 16 prefixes per mobile router. Anything beyond 16 prefixes shall be silently discarded.
  - NEMO4G-HA supports any prefix length (including /12 to /32).
  - NEMO4G-HA supports dynamic prefix updates.
    - NEMO4G-HA removes from the associated Enterprise VRF routing table any prefixes that are not included in a scheduled or ad-hoc NEMO MIPv4 re-registration request from a given MR (assuming these were present in a previous NEMO MIPv4 RRQ). HA/PGW/GGSN shall update the external VRF router of the removal of such prefixes on the next eBGP update.
    - NEMO4G-HA accepts and installs any new prefixes that are included in a scheduled or ad-hoc NEMO MIPv4 re-registration request to the associated Enterprise VRF routing table, as long as it doesn't exceed the maximum number of supported prefixes per MR (up to 16). HA/PGW/GGSN shall update the external VRF router of the newly installed prefixes on the

next eBGP update. NEMO4G-HA shall accept NEMO MIPv4 RRQs that do not include any prefixes in the first initial RRQ and it shall accept prefixes advertised in subsequent RRQs.

- In case of a prefix whose IP address or mask is changed on the MR, the MR will remove the old IP address/mask and add the new IP address/mask prefix in a scheduled or ad-hoc NEMO MIPv4 re-registration request and NEMO4G-HA shall remove the old route and add the new route corresponding to the new prefix to the Enterprise VRF routing table

- Overlapping IP addressing

  NEMO4G-HA Multi-VRF feature support private and overlapping IP addressing across multiple Enterprise network being connected from a Mobile Router. A Mobile Router (MR) can be configured with devices/subnets to seamlessly access multiple enterprise VRFs, and the network traffic targeted for those different VRFs shall share same MIP tunnel without compromising the privacy and security. Each VRF works independently through the MR and HA services.

- **Multi-VRF Support**

  The Multi-VRF Support feature enables a service provider to support two or more Virtual Private Networks (VPNs), where the IP addresses can overlap several VPNs. The Multi-VRF Support feature uses input interfaces to distinguish routes for different VPNs and forms virtual packet-forwarding tables by associating one or more interfaces with each virtual routing and forwarding (VRF) instance.

  NEMO4G-HA supports Multi-VRF within the same Mobile Router, for which the signaling and forwarding mechanism has been extended. Each enterprise network is associated with its own VRF. Both MR and HA share common vrf-names. MR and HA services are enhanced to support Cisco NVSE extension for NEMO with multiple VRF.

  Multi-VRF NEMO includes the following features:

  - A new Cisco NVSE carries VRF tags as part of the registration signaling. The Mobile Network Prefixes (MNP) are associated with these VRF tags. Furthermore, a GRE key associated with the VRF is embedded to this new NVSE, in order to provide VRF traffic segregation between the MR ISR and the NEMO-HA ASR 5500 during data forwarding. Note, there may be multiple MNPs for one GRE key, but not one MNP for multiple GRE keys.

  - The CLI config with the vrf-list and/or default VRF with IP Pool does not automatically enable multi-VRF.

    Multi-VRF takes effect only if:

    - MR sends in RRQ with the new NVSE format.
    - The specific VRF name is authorized with the ip-pool config. (the default VRF is always authorized, so vrf-list is NOT required to support multi-vrf, all the old config could support multi-vrf without any change. If an IP Pool or vrf-list is changed, it takes effect only for future new calls.

Important Next-hop forwarding is not supported by Multi-VRF with 15.0. Only MPLS is supported.

  - Home Agent on receiving the Mobile IP Registration Request from the mobile router with the above NVSE, and after a successful authentication learns about the dynamic mobile networks associated with the mobile router from the Dynamic Network extension in the Registration Request. If the

request is authorized, a Registration Reply with the Mobile Router Multi-VRF NVSE extension is sent.

- The Home Agent supports the following:
  - Dynamic Mobile Network Prefix (MNP) updates for an authorized VRF.
  - VRF addition/deletion of VRF's from the authorization list without requiring mobile pool reconfiguration.
  - MNP's of any length, including /32.
  - Geo-redundancy (ICSR) for NEMO Multi-VRF.
  - Mapping of a mobile pool to a list of authorized VRF's.
  - Multiple VRF authorization lists for 1 APN or Subscriber Profile.
- The Home Agent on receiving a packet from the tunnel shall use the GRE key for VRF forwarding the packet towards the enterprise.
- On receiving a packet from the enterprise towards the MR, the VRF key associated with the interface IDB shall be used as the GRE key.

NEMO MR Authorization

NEMO4G-HA authorizes a NEMO MIPv4 session only if a NEMO permission has been assigned to the underlying PDN connection. NEMO permission should be assigned to the underlying PDN connection through either local configuration (APN parameter) or for CDMA via subscriber profile or based on a NEMO permission AVP assigned by the 3GPP AAA during the PDN authorization. For local configuration, a new APN parameter or for CDMA via subscriber profile is supported to enable NEMO permission at the APN/PDN level within the HA/PGW/GGSN service. VRF authorization is needed. The multi-vrf authorization is done by comparing RRQ's each VRF name with the ip-pool's Default VRF or names defined by the vrf-list.

MIPv4 NEMO Protocol

NEMO4G-HA processes a Mobile IPv4 NEMO Registration Request (RRQ) received from the MR NEMO client. The RRQ shall carry multiple NVSEs to reflect the multiple VRFs and multi-tenant Prefixes per MR.

Overlapping MNPs are allowed, if they are associated with different VRF. MNP must be different if same VRF name is used on either one MR or across all MRs. Though per customer request, HA does not explicitly deny a request with such misconfiguration.

NEMO4G-HA processes the maximum of 16 Cisco-specific MIPv4 Extensions of type Normal Vendor/Org Specific Extension (NVSE) that are included in the MIPv4 NEMO RRQ. The Cisco NVSE carries VRF tags as part of the registration signaling. A GRE key associated with the VRF shall be embedded to this new NVSE, in order to provide VRF traffic segregation between the MR ISR and the NEMO-HA ASR 5500 during data forwarding. Note, there may be multiple MNPs for one GRE key, but not one MNP with multiple GREs. The Mobile Network Prefixes (MNP) will need to be associated with these VRF tags.

Cisco-specific NVSEs follow RFC 3025 "Mobile IP Vendor/Organization Specific Extensions."

GRE Encapsulation

User traffic shall be encapsulated over a GRE tunnel between the MR NEMO client and NEMO4G-HA. The IP endpoints of the GRE tunnel shall be the IPv4 assigned to the MR modem during the Enterprise PDN connection setup and the IPv4 address of the NEMO4G-HA service on the HA/PGW/GGSN.

NEMO4G-HA shall remove the GRE encapsulation before it forwards the outbound traffic towards the Enterprise VPN via the associated SGi VLAN interface. Inbound traffic received through the same SGi VLAN interface shall be encapsulated into a GRE tunnel before it's passed to the HA/PGW/GGSN service for forwarding to the MR through the proper GTP/PMIP tunnel.

Session Interactions

The following session interaction scenarios are supported between NEMO and the underlying PDN connection made over CDMA MIP or eHRPD or LTE access.

The mobile router on receiving a packet to from the tunnel shall use the GRE key to identify the tunnel instance. After decap, the packet shall be forwarded towards the mobile networks, based on the route lookup in the specific VRF context.

On receiving a packet from the mobile network, the default-route in the specific VRF context (associated with that input interface) shall be used and the packet encap shall get the correct GRE key.

In the following circumstances, NEMO4G-HA shall withdraw the associated prefix routes from the Enterprise VRF routing table, update the eBGP neighbors and free up all internal resources allocated for the underlying PDN connection and NEMO session:

- When the eHRPD terminates the underlying PDN connection (PPP-VSNCP-Term-Req sent to MR and PMIP-BU with lifetime = 0 sent to HA/PGW/GGSN).
- When the MR terminates the PPP/PDN connection when accessing the network via eHRPD.
- After an eUTRAN (LTE) detach procedure initiated by the MR or MME.

NEMO4G-HA shall not be able to process any NEMO MIPv4 RRQs if there's no underlying PDN connection associated to those RRQs (PMIPv6 or GTP). In other words, NEMO MIPv4 RRQs can be accepted and processed only if an Enterprise PDN connection has been established with HA/PGW/GGSN by the mobile router.

NEMO4G-HA shall silently ignore NEMO MIPv4 RRQs if the underlying PDN connection associated to each of those RRQs does not have the NEMO permission indication. This applies to CDMA, eHRPD and LTE access.

NEMO4G-HA shall forward (not drop) user data using MIP or GRE tunneling (UDP/434 or IP Protocol/47, respectively) to the external enterprise VRF if such data is not destined to the NEMO4G-HA IP address. This applies to PDN connections that have or do not have the NEMO Permission indication. This shall also apply to both eHRPD and LTE access.

Any failure on either the authentication or authorize of a NEMO MIPv4 session shall not affect the underlying PDN connection established between the mobile router and the HA/PGW/GGSN via eHRPD or LTE. For example, if the security credentials do not match between the MR NEMO client and NEMO4G-HA, NEMO4G-HA can reject the NEMO MIPv4 RRQ, but the associated PDN connection shall not be terminated.

NEMO Session Timers

NEMO4G-HA uses the registration lifetime value locally configured, even though MR's may use the maximum possible value (65534).

NEMO4G-HA can process ad-hoc NEMO RRQ messages.

Enterprise-wide Route Limit Control

NEMO4G-HA supports a control mechanism to limit the maximum number of prefixes/routes that a given enterprise can register, including the pools for WAN IP assignments.

When the maximum number of routes is reached, a syslog message is generated. Once the number of routes goes under the limit, a syslog message is generated for notification. And no further routes are accepted into the VRF route table. NEMO MIP RRQ is rejected accept for Multi-VRF NEMO in which case the NEMO MIP RRQ is accepted but offending VRF denied.

Forced Fragmentation

HA/PGW/GGSN forces IP packet fragmentation even for IP packets with the DF-bit set from enterprise to mobile. From mobile to enterprise DF-bit is honored.

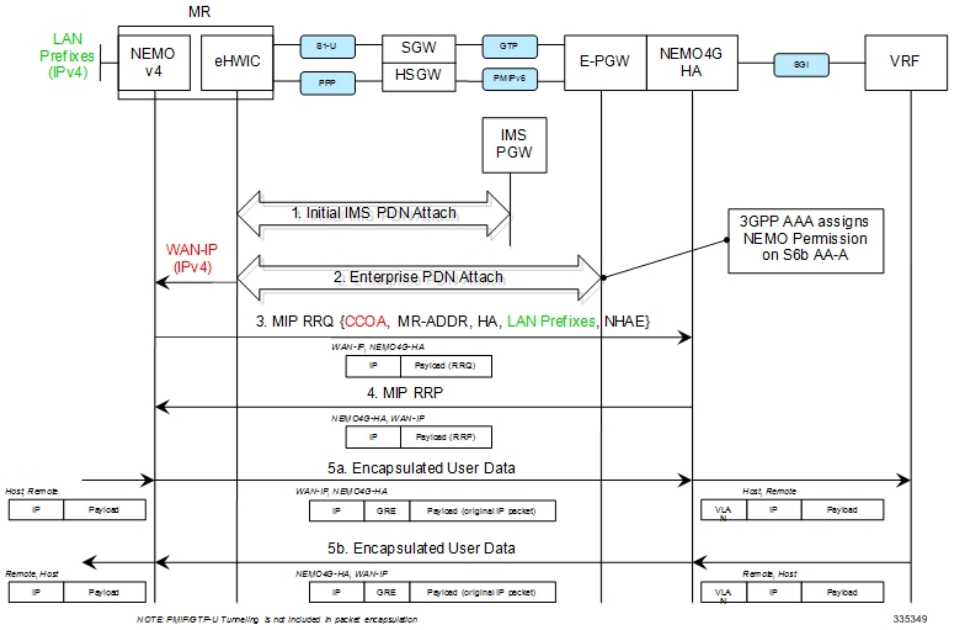
Redundancy/Reliability

CDMA, eHRPD and LTE all support intra-chassis Session Redundancy (SR) and Inter-Chassis Session Redundancy (ICSR) functionalities.

NEMO Call Flow

The following figure describes the call flow of the NEMOv4 solution.

Figure 26: NEMOv4 Call Flow



1. The Cisco MR eHWIC establishes first a connection to the IMS PDN to register to the LTE Network. The eHWIC's User Id must be properly provisioned on the HSS/SPR to be successfully authenticated.

2. After the Cisco MR eHWIC registers with the LTE network and establishes a connection to the IMS PDN, then it connects to the appropriate Enterprise PDN based on the locally configured Enterprise APN.
   - During the PDN authorization procedure using S6b, the 3GPP AAA assigns a NEMO permission via AVP. The AVP is also be available as an APN parameter on the HA/PGW/GGSN to allow NEMO service at the PDN/Enterprise level.
   - HA/PGW/GGSN assigns the MR eHWIC an IPv4 address from the Enterprise IPv4 pool assigned during PDN authentication.
   - HA/PGW/GGSN creates the proper flows internally to forward packets to the corresponding VRF external to the HA/PGW/GGSN platform using the IPv4 pool configuration on the egress context.
   - The MR eHWIC passed on the assigned IPv4 address to the NEMO application (also called WAN-IPv4 address).

3. The MR NEMO application initiates a Mobile IPv4 registration request (RRQ) using the following local configuration and the IPv4 address assigned to the eHWIC during the Enterprise PDN attach procedure (referred to as WAN-IP). The NEMO MIPv4 RRQ shall be carried as a regular user packet over the mobility connection, either GTP in LTE and PPP/PMIPv6 in eHRPD. The NEMO MIPv4 RRQ includes the following key parameters:
   - MNP - NVSE contains the Mobile Network Prefixes(MNP), a tag designating the VRF instance, and a GRE key (for downlink traffic) associated with the VRF. When the HA/PGW/GGSN receives the RRQ with the NVSE, it shall examine the MNPs. Assuming that there is no error conditions (e.g. overlapping MNPs in the same VRF), it shall insert the MNPs in the VRF routing table with the same identifier (i.e. VRF name) as the VRF tag in the NVSE. A routing entry is added to direct the downlink traffic toward each MNP to a tunnel with the GRE key, which is based on the value learned from the NVSE.
   - CCOA - IPv4 address assigned to the eHWIC modem during the Enterprise PDN connection setup (WAN-IP). The MR NEMO application will use the CCOA/WAN-IP address as the source of all NEMO packets sent to NEMO4G-HA (control and tunneled user traffic).
   - MR-HADDR - Mandatory IPv4 address preconfigured in the MR NEMO application. MR-HADDR is normally used as the source of all NEMO control packets sent to the NEMO4G-HA. However, the MR NEMO application will use the CCOA as the source for all NEMO packets (control and tunneled user traffic). Therefore, NEMO4G-HA will ignore the preconfigured MR-HADDR included in the RRQ, but it will still include it in the NEMO MIPv4 RRP.
   - Home Agent Address - Preconfigured IPv4 address that the MR NEMO application uses as the destination for all NEMO control and GRE tunneled user data (NEMO4G-HA's IPv4 Address).
   - Explicit LAN Prefixes - Locally attached IPv4 networks preconfigured on the MR NEMO application. LAN prefixes will be encoded in the same Cisco NVSE extension currently used in the NEMO solution for 3G. The Cisco NVSE included in the NEMOv4 MIP RRQ is in the form of a TLV.
   - N-MHAE - Mandatory NEMO MN-HA Authentication Extension that includes the SPI and the authenticator computed using a pre-shared Key. Both SPI and Key are preconfigured in the MR NEMO application as well.
   - NEMO-Tunnel flags such as, but not limited to, "Reverse Tunnel," "Direct Termination," "Tunnel Encapsulation" = GRE.

4. NEMO4G-HA sends a MIP registration response (RRP) back to the MR after it performs the following tasks:
   - Authenticate the RRQ using the N-MHAE information included in the RRQ.
   - Authorize the NEMO service based on the NEMO permission attribute assigned to the associated Enterprise PDN connection.
   - Accept the prefixes advertised in the Cisco NVSE extension included in the NEMO MIPv4 RRQ.
     - Confirm the MNPs are accepted in the VRF forwarding table.
     - The learned prefixes will have to adhere to the current rules of valid pool routes. The minimum valid mask length is /13 and pool routes can not include 0.0.0.0 or 255.255.255.255.
     - NEMO4G-HA will accept a minimum of 0 prefixes and a maximum of 16 prefixes. Anything beyond 16 prefixes will be silently discarded.
     - NEMO4G-HA will also check that the new resultant enterprise route count (total number of VRF routes) do not exceed the route limit potentially configured for the given enterprise. If the preconfigured route limit is exceeded, then NEMO4G-HA will reject the NEMO MIP RRQ. Otherwise, NEMO4G-HA will install the accepted prefixes in the internal VRF associated with the Enterprise PDN.
     - eBGP would then propagate the new NEMO routes to the external VRF as part of the next BGP update.

5. 1. The VRF's GRE, which is in the RRP that the MR received from HA, is used for this data packet.
   2. Upon receiving the NEMO MIP RRP, the MR will install a default route (0.0.0.0/0) in its routing table (associated with the VRF tag in the NVSE) to direct uplink traffic to a tunnel with the GRE key, which is based on the value learned from the NVSE, to route all traffic through the CDMA/LTE/GGSN connection. The VRF's GRE that is contained in the RRQ to HA from MR is used to wrap the data.
      - Outbound packets are encapsulated over GRE using the CCOA/WAN-IP address as the source and the NEMO4G-HA-Service IPv4 address as the destination of the tunnel.
      - Inbound packets are encapsulated over GRE as well from the NEMO4G-HA to the MR NEMO application. The source of the GRE tunnel is the NEMO4G-HA-Service IPv4 address and the destination is the CCOA/WAN-IP address.

Fault and Fault Reporting

HA tries to accommodate the variety of RRQ without issuing failures. However, if failure occurs, different level of logging message are logged And the E-XGW will return RRP with error code 0 but not include the failed VRFs or MNPs.

Multi-VRF error handling is close to non-VRF environment. However, the following scenarios are considered as errors:

- **MR is not authorized for NEMO service, but has valid security association:**

  If the MR is not authorized for the NEMO service, but has a valid security association. HA/PGW/GGSN shall silently discard the registration request.

- **Misconfiguration or unauthorized VRF:**

  There may be an issue with a single VSE due to misconfiguration of a VRF name or simply the VRF may not be authorized. Upon receipt of the MR RRQ, the HA/PGW/GGSN shall reply with RRP, with status value of 0 (Accepted), but the NVSE for the failed VRF shall not be included in the reply. The missing NVSE in the RRP serves as a hint to the MR that the given VRF was not accepted. This behavior allows the other VRFs to be accepted (status code 0) and unaffected by the errant VSE.

  The MR shall set up forwarding only for the accepted VPN/subnets. It shall not set up tunnel forwarding for the rejected VPN/prefixes.

  MR shall continue to include all the VSE's in the subsequent re-registration RRQ, including the customer VRF that was not in the previous RRP response.

  Where ALL NVSEs are problematic, if the status code remains as 0 (Acccepted) with no NVSE included in the NEMO MIP RRP, the status code shall not revert to 129.

- **Single VRF exceeds the maximum route-limit at HA/PGW/GGSN:**

  A Multi-VRF enabled Mobile Router registers NVSEs, and a specific VSE is carrying MNPs which exceeds the total maximum configurable route-limit for associated VRF at the HA/PGW/GGSN. In this particular case, the HA/PGW/GGSN shall respond with status code of 0 (Accepted) in the RRP, but the problematic NVSE shall not be included in the RRP reply. The missing RRP provides hint there was a problem with the VRF.

- **A single MR attempts to register more than 16 MNPs:**

  If more than 16 MNPs are configured for MR registration, the HA/PGW/GGSN shall accept the partial prefix set, up to 16. The accepted MNPs are echoed in the RRP.

Important ASR 5500 NEMO HA dynamically updates the VRF routing tables accordingly by processing ONLY the first 16 MNPs in the RRQ. Because the ordering of the MNPs in RRQ may not be ensured by MR, every time, a different set of 16 MNPs MAY be registered by ASR 5500 NEMO HA.

Errors Pertaining to VRFs: The error message does not indicate which VRF has caused the failure. To know the VRF that has caused the failure, print all the requesting VRFs for errors. A denied VRF does not result in a RRQ failure if the other VRFs are accepted. The following scenarios, but not limited to, are considered as failures:

- IP pool refers to a named **framed-route-vrf-list**, but there is no **vrf-list** defined in the context.
- The context defined **vrf-list** with a named VRF, but no vrf is defined with that name.
- The context defined **vrf-list** with more than 16 VRF names.
- The RRQ NVSE contains a VRF that is neither the Default VRF on HA, nor in the **framedrouter-vrf-list**. A default VRF of IP pool is specified by its **vrf** parameter.
- The RRQ NVSE contains a VRF name longer than 63 bytes. The VPN system pre-allocated 64 bytes for the NULL terminated string. The error for the VRF name that is longer than 63 bytes is returned.

The following scenarios are not considered as errors, as HA is able to make a decision and achieve the best usability:

- IP pool does not define a value for **vrf** parameter, whether a **framed-route-vrf-list** is specified or not. The value specified by IP pool\'s **vrf** parameter is called Default VRF, where IP address is advertised in when the input **vrf** is unnamed. When this parameter is not specified, Default VRF is its current context.

- The RRQ NVSE contains a VRF without a name, or empty name. All the prefixes in this VRF are treated as for the implied Default VRF in the IP Pool.
- The RRQ NVSE contains a VRF name that matched with the Default VRF but is not a member of the **framed-router-vrf-list**. This is due to the fact that the Default VRF is always authorized.
- The RRQ contains more than 16 prefixes in total, regardless of how many VRFs are they in. HA will ignore those prefixes after 16. This ensures that the existing non-vrf or unnamed vrf features are unaffected.
- When IP pool does not specify the **framed-router-vrf-list** parameter or list is specified but empty, both work with the current behavior. The following special rules apply:
  - RRQ NVSE may contain no VRF. Then no authorization will take place, the Default VRF will be directly used for IP pool.
  - RRQ NVSE contains only one VRF which has the **vrf** setting for authorization. The Default VRF is used to advertise the IP address.

Engineering Rules

- Up to 300 virtual routing tables per context and 64 BGP peers per context.
- Up to 5k host routes spread across multiple VRFs per BGP process. Limited to 6000 pool routes per chassis.
- Upto 2048 VRFs per chassis
- Per MR:
  - 0~16 VRF per one MR/CPE
  - One NVSE per one VRF
  - Upto 16 MNPs per VRF
- 1~16 VRF per one vrf-list
- 0~63 bytes VRF names in ASCII text

Supported Standards

- IETF RFC 5177 (April 2008) "Mobile IPv4 NEMO Extensions,"
- IETF RFC 3025 (February 2001) "Mobile IP Vendor/Organization Specific Extensions"
- IETF RFC 3115 (April 2001) "Mobile IP Vendor/Organization Specific Extensions"

Configuring NEMOv4 Multi VRF

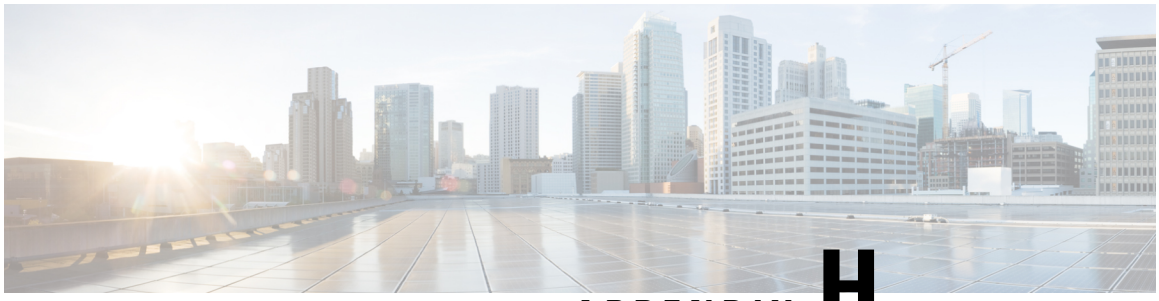
ASR 5500 provides some CLI commands with this new feature.

NEMO Multi-VRF Egress

```
config
   context <egress1>
      ip vrf <vrf-name1>
         ip maximum-routes 4998
      exit
```

NEMOv4 with Multi-VRFs

```
        ip vrf <vrf-name2>
           ip maximum-routes 4998
        exit
        ip vrf <vrf-name3>
           ip maximum-routes 4998
        exit
        ip vrf-list <vrf_list_1> permit <vrf-name1>
        ip vrf-list <vrf_list_1> permit <vrf-name2>
        ip vrf-list <vrf_list_1> permit <vrf-name3>
        mpls bgp forwarding
        ip pool <poolname1-b> <ipaddress> private 0 srp-activate group-name
<customer1> vrf <vrfname1> policy policy framed-route-vrf-list <vrf_list_1>
allow-static-allocation
        router bgp 1
           router-id <ipaddress>
           neighbor <ipaddress> remote-as 1001
           neighbor <ipaddress> remote-as 1001
           address-family <vpnv4>
              neighbor <ipaddress> activate
              neighbor <ipaddress> send-community both
              neighbor <ipaddress> activate
              neighbor <ipaddress> send-community both
           exit
           ip vrf <vrfname1>
              route-distinguisher 1 1
             route-target export 1 1
               route-target import 1 1
        exit
        address-family ipv4 vrf  <vrfname1>
           redistribute connected
           redistribute static
        exit
        ip vrf <vrfname2>
           route-distinguisher 2 2
           route-target export 2 2
           route-target import 2 2
        exit
        address-family <ipv4> vrf <vrfname2>
             redistribute connected
             redistribute static
         exit
        ip vrf <vrfname3>
           route-distinguisher 3 3
           route-target export 3 3
           route-target import 3 3
        exit
          address-family <ipv4> vrf <vrfname3>
            redistribute connected
            redistribute static
          exit
```



APPENDIX H

IP Network Enabler

This chapter describes the StarOS IP Network Enabler (IPNE) feature. It describes how the feature works, and how to configure and monitor IPNE.

Feature Description

This section provides a description of the IPNE feature.

IPNE (IP Network Enabler) is a MINE client component running on various network nodes within operator's network (P-GW, GGSN, HA, or HNBGW), to collect and distribute session/network information to MINE servers. The MINE cloud service provides a central portal for wireless operators and partners to share and exchange session and network information to realize intelligent services.

The information is shared between the MINE server and IPNE service in the form of XML data. The core object in the IPNE service is the XMPP protocol engine. There is one XMPP protocol engine instance for each configured MINE server peer. The engine implements the XMPP protocol using FSM.

All information that is shared is derived from the context at that instance in time. An IPNE service level scheduler is also implemented to rate-control the feed and notification activities on all the handles to avoid overload which would affect call processing and data path performance.

Relationships to Other Features

This section describes how the IPNE service is related to other features.

One of the following GW services must be configured on the StarOS before IPNE can be configured:

- GGSN
- HA
- HNBGW
- P-GW

Refer to the *GGSN Administration Guide*, the *HA Administration Guide*, the *HNBGW Administration Guide* and the *P-GW Administration Guide* for configuration procedures.

The MINE cloud service provides a central portal for wireless operators and partners to share and exchange session/network information to realize intelligent services. A MINE client component is running on various network nodes within operator's network, e.g. PGW, HA, to collect and distribute session/network information to MINE servers. The client is IPNE.

The IPNE client runs on the StarOS as a configurable service. The Enhanced Charging Service (ECS) component interacts with the IPNE client in order to fulfill the defined requirements.

For best IPNE performance, the ECS component should provide the following functionality:

- Flow information parameters should be provided by ECS to IPNE:
  - Tuple information
  - URL
  - User Agent
  - Application protocol
  - Flow creation time

NBR information parameters should be provided by ECS to IPNE:

- NAT-IP address
- Start Port
- End Port

ECS should provide the above parameters for all active flows in a response corresponding to the query from the MINE server indexed on the subscriber's call id.

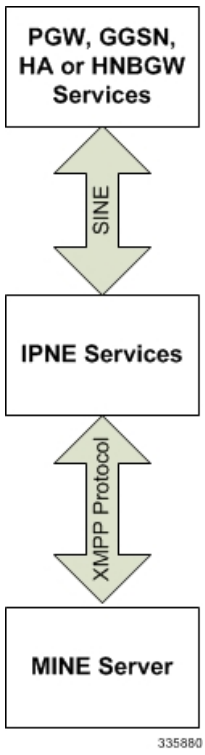
For the subscription that is installed by the IPNE client on a subscriber's call id, ECS should send a notification message to the IPNE client whenever a subscribed trigger is detected.

How it Works

IPNE

The following diagram describes the architecture for the IPNE interface. The session manager and IPNE will interact via the SINE interface. The information will be exchanged between the modules in the form of clp handles. For each session one IPNE handle is created. The information is stored in a local database on the IPNE client side.

Figure 27: High-Level IPNE Architecture



The interaction takes place at the time of:

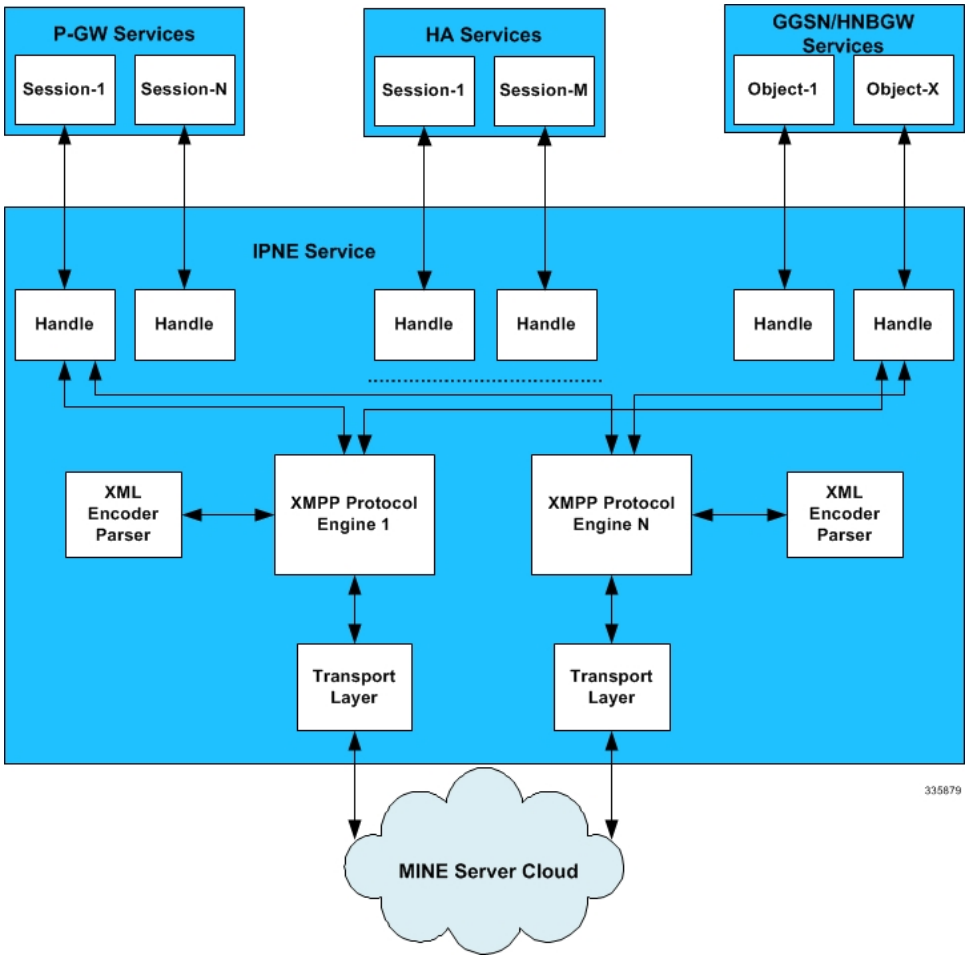
- Session setup so as to add the session information at the IPNE side
- To pass the feed messages to the MINE server
- While responding to the query request sent by the MINE server.
- Subscription notification from IPNE client to MINE server

The MINE server and IPNE client interact with each other for all procedures using the XMPP protocol over the SINE interface. The information stored at the IPNE client side is converted to XML format and then passed on to the MINE server. Upon receiving the messages (query requests) from the MINE server, IPNE decodes it and sends the corresponding clp handle to the session manager. The information that is shared is a snapshot of the session/flow/nbr context at that instance in time.

Architecture

The MINE IPNE client is implemented as a configurable service on P-GW, HA, GGSN or HNBGW services as illustrated below.

Figure 28: Detailed IPNE Architecture



Limitations

Note the following limitations for the IPNE feature:

- The IPNE service implements a flow control mechanism over the XMPP interface. As a result, any messaging over this interface which exceeds the set queue thresholds would be discarded.

Flows

This section provides call flow diagrams for IPNE Query, Subscription, Feed, Addition and Deletion scenarios. Some flow diagrams use the P-GW as an example, but they also apply to GGSN, HA, and HNBGW as well.

Figure 29: IPNE Handling of Query from MINE Server

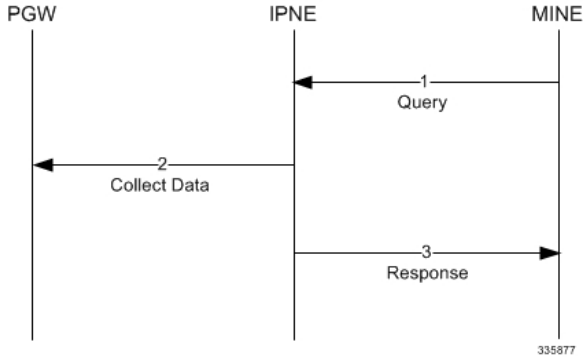


Table 25: IPNE Handling of Query from MINE Server

Step	Description
1	The MINE server sends a query over the XMPP stream to the IPNE service. The query is XML encoded, which contains a query-id, key to look up a session (for example, sessmgr instance:callid), and a list of segments specifying the interested information.
2	Upon receipt of the query, the IPNE service parses the XML data and finds the handle using the key provided by MINE server, and then invokes the registered call back function to collect the session information. The requested information is also provided to the call back function in the form of a bit mask.
3	With the help of XML encoder, the IPNE service converts the session information to XML format and sends it to the MINE server.

Figure 30: IPNE Service Handling a Subscription from the MINE Server

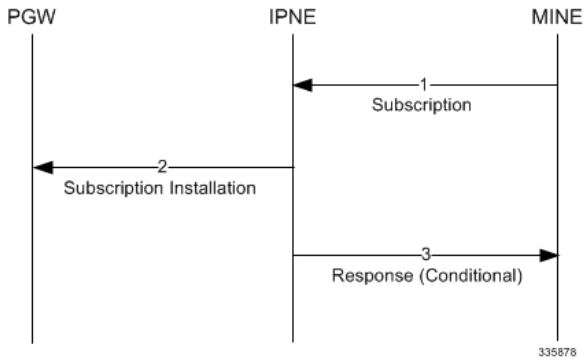


Table 26: IPNE Service Handling a Subscription from the MINE Server

Step	Description
1	The MINE server sends a subscription over the XMPP stream to the IPNE service. The subscription is XML-encoded and has a similar format as the query message, e.g. a list of fragments specifying the feed triggers.
2	The subscription installation is maintained by the IPNE on a per handle basis.
3	This step is conditional. If there are any existing sessions that match any of the triggers listed in the subscription, A success acknowledgement message is sent to the MINE server.

Figure 31: IPNE Service Sends Unsolicited Feed Message to the MINE Server

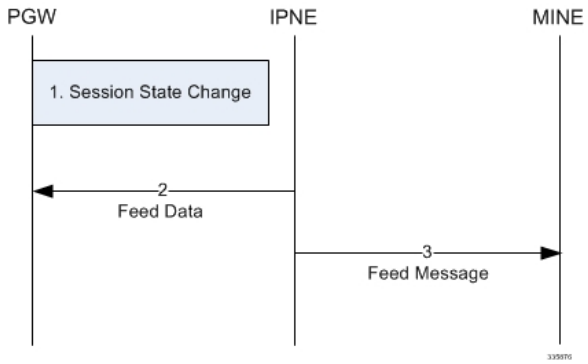


Table 27: IPNE Service Sends Unsolicited Feed Message to the MINE Server

Step	Description
1	A session detects some state change, for example, a RAT change due to a handoff.
2	The session invokes a public API on the handle to inform the IPNE service of the change.
3	If the change matches any of the subscription installations installed on the IPNE handle, a feed message is built and sent to the MINE server(s).

Figure 32: IPNE Session Addition

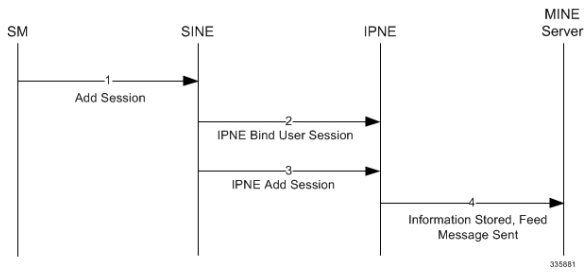


Table 28: IPNE Session Addition

Step	Description
1	While setting up the session, the session manager application checks to see if IPNE is enabled.
2	If IPNE is enables, the SM sends the add session information to the SINE interface.
3	SINE binds the session information and sends the add event towards the IPNE application.
4	Information is stored, and the information is passed as a feed message to the MINE server in the form of XML data.

Figure 33: IPNE Session Deletion

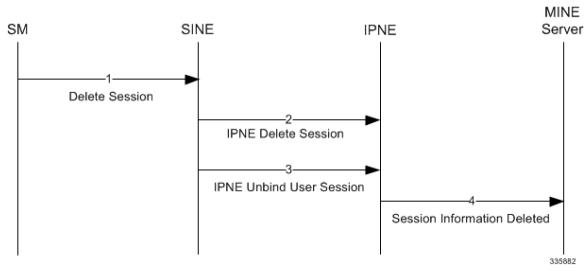


Table 29: IPNE Session Deletion

Step	Description
1	Before releasing the session, the session manager application calls for delete_session.
2	SINE invokes the delete session event.
3	SINE unbinds the session information.
4	The corresponding session information is deleted from the IPNE application and a feed message is sent to the MINE server with type as delete.

Standards Compliance

The StarOS IPNE feature complies with the following standards:

- RFC 6120; Extensible Messaging and Presence Protocol (XMPP): Core, Section 4.7 (Stream attributes)

Configuring the IPNE Feature

This section describes how to configure the IPNE feature and how to verify the configuration.

Configuring IPNE

This section describes how to configure the IPNE feature.

Configuring IPNE includes configuring the IPNE service, and then associating the IPNE service with the GGSN, HA, HNBGW or P-GW service.

Use the following example configuration to create the IPNE service.

```
config
 context context_name
 ipne ipne_service_name
 ipne-endpoint
 bind [ ipv4 ipv4_address | ipv6 ipv6_address ]
 peer [ ipv4 | ipv6 ] protocol tcp
 end
```

Notes:

- Both the **bind** and **peer** keywords support IPv4 and IPv6 addressing.
- **tcp** is the default transport protocol. SCTP is not supported at this time.
- The default XMPP protocol port is 5222.
- The **fqdn**, **priority** and **weight** keywords are not supported at this time.

HNBGW only. Usually, notify messages are sent only on subscription. However, an exception has been made for HNBGW UE Registration / Deregistration. HNBGW UE Registration/Deregistration will always be notified without any subscription. To control the sending of such unsolicited notification, enter the following command:

```
configure
      context ipne_service_name
            unsolicited-notify-trigger hnb-ue
            end
```

Notes

- If **unsolicited-notify-trigger hnb-ue** is configured, the IPNE service sends notifications for UE Register/De-register requests on receiving the requests from the HNBGW.
- If **no ununsolicited-notify-trigger hnb-ue** is configured, the IPNE will not send UE Register/De-register notifications. This is the default setting.

Once the IPNE service has been created, it must be associated with the configured GGSN, HA, P-GW or HNBGW service. Use the following example to associate the IPNE service with the configured gateways service

```
configure
      context gw_context_name
 associate ipne-service ipne_service_name
           end
```

Notes:

- **context** *gw_context_name* is the name of the configured GGSN, HA, P-GW or HNBGW service name configured on the StarOS
- To remove the association between the IPNE service and the gateway service, use the **no associate ipne-service**command.

Verifying the IPNE Configuration

This section describes how to verify the IPNE configuration

From exec mode issue the following command to verify the IPNE configuration:

```
show ipne peers all
```

The output of this command provides the following information for each IPNE service instance:

- IPNE Service Name
- Context ID
- Peer IP address
- State of the TCP connections to the peer.

Monitoring the IPNE Service

This section describes how to monitor the StarOS IPNE feature.

IPNE Show Commands

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

The show commands in this section are available in support of the the StarOS IPNE feature.

show ipne peers all

This command provides a list of peers of each IPNE service and the state of the TCP connections.

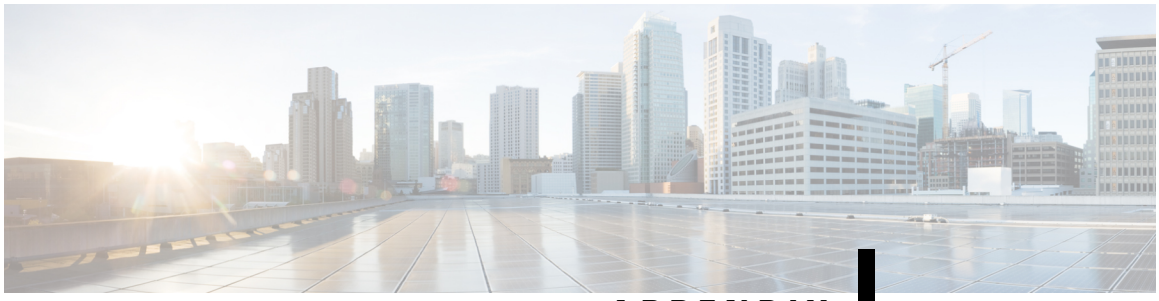
show ipne statistics all

This command shows the total number of handles for each IPNE service and counter totals for queries, responses, subscriptions and feeds.

show active-charging subscsribers full all

This command shows if the MINE server has currently subscribed notifications for this ACS session or not (**IPNE enabled** or **disabled**). It also indicates the number of notifications sent to the MINE server for this

ACS session. Historical notification counts across all current and deleted flows are stored. If the MINE server has not been subscribed for notifications, this field reads **n/a**.



APPENDIX

Intelligent Traffic Control

Before using the procedures in this chapter, it is recommended that you select the configuration example that best meets your service model, and configure the required elements as per that model.

This chapter contains the following topics:

Overview

Intelligent Traffic Control (ITC) enables you to configure a set of customizable policy definitions that enforce and manage service level agreements for a subscriber profile, thus enabling you to provide differentiated levels of services for native and roaming subscribers.

In 3GPP2 service ITC uses a local policy look-up table and permits either static EV-DO Rev 0 or dynamic EV-DO Rev A policy configuration.

Important ITC includes the class-map, policy-map and policy-group commands. Currently ITC does not include an external policy server interface.

ITC provides per-subscriber/per-flow traffic policing to control bandwidth and session quotas. Flow-based traffic policing enables the configuring and enforcing bandwidth limitations on individual subscribers, which can be enforced on a per-flow basis on the downlink and the uplink directions.

Flow-based traffic policies are used to support various policy functions like Quality of Service (QoS), and bandwidth, and admission control. It provides the management facility to allocate network resources based on defined traffic-flow, QoS, and security policies.

ITC and EV-DO Rev A in 3GPP2 Networks

Important The Ev-Do Rev 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*.

You can configure your system to support both EV-DO Rev A and ITC. ITC uses flow-based traffic policing to configure and enforce bandwidth limitations per subscriber. Enabling EV-DO Rev A with ITC allows you to control the actual level of bandwidth that is allocated to individual subscriber sessions and the application flows within the sessions.

For more information on EV-DO Rev A, refer to the *Policy-Based Management and EV-DO Rev A* chapter. For setting the DSCP parameters to control ITC functionality, refer to the *Traffic Policy-Map Configuration Mode Commands* chapter in the *Command Line Reference*.

Bandwidth Control and Limiting

Bandwidth control in ITC controls the bandwidth limit, flow action, and charging action for a subscriber, application, and source/destination IP addresses. This is important to help limit bandwidth intensive applications on a network. You can configure ITC to trigger an action to drop, lower-ip-precedence, or allow the flow when the subscriber exceeds the bandwidth usage they have been allotted by their policy.

Licensing

The Intelligent Traffic Control 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*.

How it Works

ITC enables you to configure traffic policing on a per-subscriber/per-flow basis with the potential to manipulate Differentiated Services Code Points (DSCPs), queue redirection (for example, move traffic to a Best Effort (BE) classification), or drop profile traffic.

In flow-based traffic policies, policy modules interact with the system through a set of well defined entry points, provide access to a stream of system events, and permit the defined policies to implement functions such as access control decisions, QoS enforcement decisions, etc.

Traffic policing can be generally defined as

policy: condition >> action

- **condition**: Specifies the flow-parameters like source-address, destination-address, source-port, destination-port, protocol, etc. for ingress and/or egress packet.

- **action**: Specifies a set of treatments for flow/packet when condition matches. Broadly these actions are based on:
  - Flow Classification: Each flow is classified separately on the basis of source-address, destination-address, source-port, destination-port, protocol, etc. for ingress and/or egress packet. After classification access-control allowed or denied by the system.
  - QoS Processing for individual flow and DSCP marking: Flow-based traffic policing is implemented by each flow separately for the traffic-policing algorithm. Each flow has its own bucket (burst-size) along with committed data rate and peak data rate. A Token Bucket Algorithm (a modified trTCM) [RFC2698] is used to implement this flow-based QoS traffic policing feature.

    Refer to the *Traffic Policing and Shaping* chapter for more information on Token Bucket Algorithm.

Configuring Flow-based Traffic Policing

Traffic Policing is configured on a per-subscriber basis for either locally configured subscribers on the system or subscriber profiles configured on a remote RADIUS server.

Flow-based traffic policy is configured on the system with the following building blocks:

- Class Maps: The basic building block of a flow-based traffic policing. It is used to control over the packet classification.
- Policy Maps: A more advanced building block for a flow-based traffic policing. It manages admission control based on the Class Maps and the corresponding flow treatment based on QoS traffic-police or QoS DSCP marking.
- Policy Group: This is a set of one or more Policy Maps applied to a subscriber. it also resolves the conflict if a flow matches to multiple policies.

This section provides instructions for configuring traffic policies and assigning to local subscriber profiles on the system.

For information on how to configure subscriber profiles on a remote RADIUS server, refer to the *StarentVSA* and *StarentVSA1* dictionary descriptions in the *AAA and GTP Interface Administration and Reference*.

Important This section provides the minimum instruction set for configuring flow-based traffic policing on an AGW service. Commands that configure additional properties are provided in the *Command Line Interface Reference*.

These instructions assume that you have already configured the system-level configuration as described in product administration guide.

To configure the flow-based traffic policing on an AGW service:

1. Configure the traffic class maps on the system to support flow-based traffic policing by applying the example configuration in Configuring Class Maps, on page 314.
2. Configure the policy maps with traffic class maps on the system to support flow-based traffic policing by applying the example configuration in Configuring Policy Maps, on page 314.
3. Configure the policy group with policy maps on the system to support flow-based traffic policing by applying the example configuration in Configuring Policy Groups, on page 315.

4. Associate the subscriber profile with policy group to enable flow-based traffic policing for subscriber by applying the example configuration in Configuring a Subscriber for Flow-based Traffic Policing, on page 316.
5. Verify your flow-based traffic policing configuration by following the steps in Verifying Flow-based Traffic Policing Configuration, on page 316.
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*.

Configuring Class Maps

This section describes how to configure Class Maps on the system to support Flow-based Traffic Policing.

Important In this mode classification match rules added sequentially with **match** command to form a Class-Map. To change and/or delete or re-add a particular rule user must delete specific Class-Map and re-define it.

```
configure
     context <vpn_context_name> [ -noconfirm ]
          class-map name <class_name> [ match-all | match-any ]
               match src-ip-address <src_ip_address> [ <subnet_mask> ]
               match dst-ip-address <dst_ip_address> [ <subnet_mask> ]
               match source-port-range <initial_port_number> [ to
<last_port_number> ]
              match dst-port-range <initial_port_number> [ to <last_port_number>
 ]
               match protocol [ tcp | udp | gre | ip-in-ip ]
               match ip-tos <service_value>
               match ipsec-spi <index_value>
               match packet-size [ gt | lt ] <size>
               end
```

Notes:

- <*vpn_context_name*> is the name of the destination context in which you want to configure the flow-based traffic policing.
- <*class_name*> is the name of the traffic class to map with the flow for the flow-based traffic policing. A maximum of 32 class-maps can be configured in one context.
- For description and variable values of these commands and keywords, refer to the *Class-Map Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

Configuring Policy Maps

This section provides information and instructions for configuring the policy maps on the system to support flow-based traffic policing.

```
configure
     context <vpn_context_name>
          policy-map name <policy_name>
               class <class_name>
               type { static | dynamic }
               access-control { allow | discard }
               qos traffic-police committed <bps> peak <bps> burst-size
<byte> exceed-action { drop | lower-ip-precedence | allow } violate-action
 { drop | lower-ip-precedence | allow }
               qos encaps-header dscp-marking [ copy-from-user-datagram
| <dscp_code> ]
               end
```

Notes:

- <*vpn_context_name*> is the name of the destination context in which is configured during Class-Map configuration for flow-based traffic policing.
- <*policy_name*> is the name of the traffic policy map you want to configure for the flow-based traffic policing. A maximum of 32 policy maps can be configured in one context.
- <*class_name*> is the name of the traffic class to map that you configured in *Configuring Class Maps* section for the flow-based traffic policing.
- For description and variable values of these commands and keywords, refer to the *Traffic Policy-Map Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

Configuring Policy Groups

This section provides information and instructions for configuring the policy group in a context to support flow-based traffic policing.

```
configure
     context <vpn_context_name>
          policy-group name <policy_group>
               policy <policy_map_name> precedence <value>
               end
```

Notes:

- <*vpn_context_name*> is the name of the destination context which is configured during Class-Map configuration for flow-based traffic policing.
- <*policy_group*> is name of the traffic policy group of policy maps you want to configure for the flow-based traffic policing. A maximum of 32 policy groups can be configured in one context.
- <*policy_map_name*> is name of the traffic policy you configured in *Configuring Policy Maps* section for the flow-based traffic policing. A maximum of 16 Policy Maps can be assigned in a Policy Group.
- For description and variable values of these commands and keywords, refer to the *Traffic Policy-Map Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

Configuring a Subscriber for Flow-based Traffic Policing

This section provides information and instructions for configuring the subscriber for Flow-based Traffic Policing.

```
configure
     context <vpn_context_name>
          subscriber name <user_name>
               policy-group <policy_group> direction [ in | out ]
               end
```

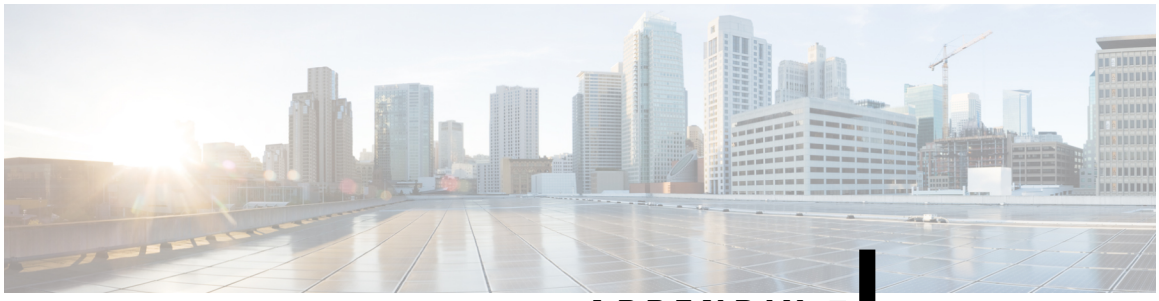
Notes:

- <*vpn_context_name*> is the name of the destination context configured during Class-Map configuration for flow-based traffic policing.
- <*user_name*> is the name of the subscriber profile you want to configure for the flow-based traffic policing.
- <*policy_group*> is name of the traffic policy group you configured in *Configuring Policy Groups* section for the flow-based traffic policing. A maximum of 16 Policy groups can be assigned to a subscriber profile.
- For description and variable values of these commands and keywords, refer to the *Traffic Policy-Group Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

Verifying Flow-based Traffic Policing Configuration

Verify that your flow-based traffic policing is configured properly by entering the following command in Exec Mode:
show subscribers access-flows full

The output of this command displays flow-based information for a subscriber session.



APPENDIX J

MIP NAT Traversal

This chapter describes support for MIP NAT traversal and how to enable it on the system. 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 the respective product Administration Guide, before using the procedures in this chapter.

Important Use of MIP NAT traversal requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

Overview

If a Mobile Node (MN) supports Mobile IP Network Address Translation (MIP NAT) traversal, it can indicate to the Home Agent (HA) that it is able to use MIP UDP tunneling when the HA sees that the Registration Request (RRQ) has traversed a NAT device.

The HA determines that the RRQ has passed through a NAT device by comparing the care-of-address in the RRQ with the source IP address of the RRQ. If they are different, and the D bit is set in the RRQ, then it indicates that the RRQ has passed through a NAT device.

If NAT is not detected but the Force (F) bit is set in the RRQ along with a UDP Tunnel Request, the HA rejects the call with the code 129 in the Registration Response (RRP). You can configure a parameter to force the HA to accept these types of requests for UDP tunneling in the absence of NAT.

When the D bit is not set and a mismatch occurs between the source address and the care-of-address, this could be a case when a mobile is registering through an FA using different addresses for signaling and data traffic. This registration behavior is allowed by the HA service.

The MN and HA negotiate UDP tunneling support during Mobile IP call setup. The MN includes a UDP Tunnel Request Extension in the RRQ sent to the HA. This extension optionally specifies the encapsulation type to be used as well (IP, GRE, or Minimal IP). The system only supports IP encapsulation at this time. Note also that the D bit must be set when UDP Tunneling is requested.

If the HA supports the requested form of tunneling, and the registration is successful, it responds with a UDP Tunnel Reply Extension in the RRP and specifies the keepalive interval the MN should use.

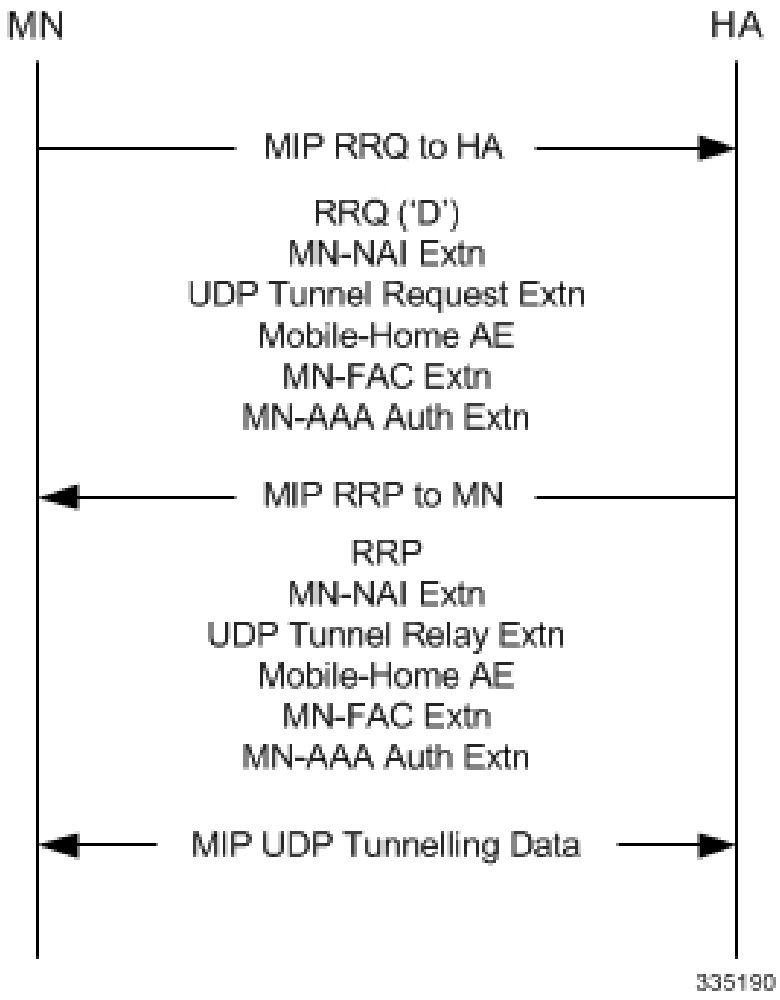
If HA does not accept the requested type of UDP tunneling, it ignores the UDP Tunnel Request extension and does not include the UDP Tunnel Reply extension in the Registration Reply. Error code 142 is used in the RRP to indicate to the MN that the requested UDP tunnel encapsulation is unavailable.

The UDP Tunnel Request extension is included in all initial, renewal, and handoff RRQ and RRP messages. The UDP Tunnel Request extension is not included in a Deregistration RRQ from the MN and the HA ignores them if they are included in Dereg RRQs received.

When MIP NAT Traversal is used, normally reverse tunneling is also used. However, this is not required by the HA.

An example of successful MIP UDP Tunneling negotiation is shown below.

Figure 34: MIP UDP Tunneling negotiation between MN and HA



The following table lists the various cases possible in UDP Tunneling negotiation during Mobile IP call establishment.

Table 30: MIP UDP Tunneling Negotiation Cases

Case	RRQ received at the HA	Action at HA
1	NAT detected, UDP Tunnel Request sent, NAT Traversal enabled	Accept call with IP-UDP tunneling, UDP Tunnel Reply included in RRP
2	NAT detected, UDP Tunnel Request sent, NAT Traversal disabled at the HA	Reject with code 129
3	NAT not detected, UDP Tunnel Request sent, F bit not set	Accept call with IP-IP tunneling, UDP Tunnel Reply not included
4	NAT not detected, UDP Tunnel Request sent, F bit set, forced UDP tunnel NOT allowed	Reject with code 129
5	NAT not detected, UDP Tunnel Request sent, F bit set, forced UDP tunnel allowed	Accept call with IP-UDP tunneling, UDP Tunnel Reply included in RRP
6	UDP Tunnel Request sent, D bit not set	Reject with code 134
7	NAT detected, UDP Tunnel Request not sent	Reject with code 129

Enabling MIP NAT Traversal

MIP NAT traversal must be enabled for the desired HA service on the system.

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

To enable MIP NAT traversal, set parameters by applying the following example configuration:

```
configure
 context <context_name>
 ha-service <name>
 nat-traversal
 end
```

Notes:

- Optionally, you can configure the HA to accept requests when NAT is not detected but the Force (F) bit is set in the RRQ with the UDP Tunnel Request by entering the following command: **nat-traversal force-accept**

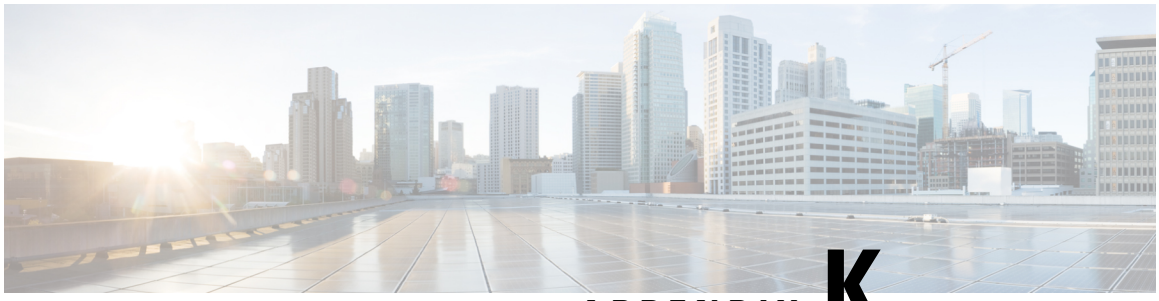
Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Viewing MIP NAT Traversal Statistics

Use the following commands in **exec mode** to list statistics that include information about MIP NAT Traversal:

- **monitor {protocol | subscriber}**- Use the MIP Tunnel option to trace IP-UDP tunneled datagrams.
- **show ha-service** *service_name* - Shows the MIP NAT Traversal configuration for the specified HA service.
- **show mipha statistics** - Lists IP-UDP tunnel statistics for Home Agent calls specified.
- **show mipha full** - Displays NAT, UPD, and encapsulation information for Home Agent calls specified.
- **show subscribers full** - Displays NAT, UPD, and encapsulation information for the subscribers specified.
- **{show | clear} subscribers ccoa-only** - Show or clear sessions for subscribers that registered a MIP colocated COA directly with the HA.
- **{show | clear} subscribers mip-udp-tunnel-only** - Show or clear sessions for subscribers that negotiated MIP UDP tunneling with the HA.

Refer to *Exec Mode Commands* chapter in the*Command Line Interface Reference* for details on using these commands.



APPENDIX K

Mobile IP Registration Revocation

This chapter describes Registration Revocation for Mobile-IP and Proxy Mobile-IP and explains how it is configured. 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 This license is enabled by default; however, not all features are supported on all platforms and other licenses may be required for full functionality as described in this chapter.

This chapter includes the following topics:

Overview

Registration Revocation is a general mechanism whereby either the HA or the FA providing Mobile IP functionality to the same mobile node can notify the other mobility agent of the termination of a binding. This functionality provides the following benefits:

- Timely release of Mobile IP resources at the FA and/or HA
- Accurate accounting
- Timely notification to mobile node of change in service

Mobile IP Registration Revocation can be triggered at the FA by any of the following:

- Session terminated with mobile node for whatever reason
- Session renegotiation
- Administrative clearing of calls
- Session Manager software task outage resulting in the loss of FA sessions (sessions that could not be recovered)

Important Registration Revocation functionality is also supported for Proxy Mobile IP. However, only the HA can initiate the revocation for Proxy-MIP calls.

Mobile IP Registration Revocation can be triggered at the HA by any of the following:

- Administrative clearing of calls
- Inter-Access Gateway handoff. This releases the binding at the previous access gateway/FA
- Session Manager software task outage resulting in the loss of FA sessions (for sessions that could not be recovered)
- Session Idle timer expiry (when configured to send Revocation)
- Any other condition under which a binding is terminated due to local policy (duplicate IMSI detected, duplicate home address requested, etc.)

The FA and the HA negotiate Registration Revocation support when establishing a Mobile IP call. Revocation support is indicated to the Mobile Node (MN) from the FA by setting the 'X' bit in the Agent Advertisement to MN. However the MN is not involved in negotiating the Revocation for a call or in the Revocation process. It only gets notified about it. The X bit in the Agent Advertisements is just a hint to the MN that revocation is supported at the FA but is not a guarantee that it can be negotiated with the HA

At the FA, if revocation is enabled and a FA-HA SPI is configured, the Revocation Support extension is appended to the RRQ received from the MN and protected by the FA-HA Authentication Extension. At the HA, if the RRQ is accepted, and the HA supports revocation, the HA responds with an RRP that includes the Revocation Support extension. Revocation support is considered to be negotiated for a binding when both sides have included a Revocation Support Extension during a successful registration exchange.

Important The Revocation Support Extension in the RRQ or RRP must be protected by the FA-HA Authentication Extension. Therefore, an FA-HA SPI must be configured at the FA and the HA for this to succeed.

If revocation is enabled at the FA, but an FA-HA SPI is not configured at the FA for a certain HA, then FA does not send Revocation Support Extension for a call to that HA. Therefore, the call may come up without Revocation support negotiated.

If the HA receives an RRQ with Revocation Support Extension, but not protected by FA-HA Auth Extension, it will be rejected with "FA Failed Authentication" error.

If the FA receives a RRP with Revocation Support Extension, but not protected by FA-HA Auth Extension, it will be rejected with "HA Failed Authentication" error.

Also note that Revocation support extension is included in the initial, renewal or handoff RRQ/RRP messages. The Revocation extension is not included in a Deregistration RRQ from the FA and the HA will ignore them in any Deregistration RRQs received.

Configuring Registration Revocation

Support for MIP Registration Revocation requires the following configurations:

- **FA service(s):** Registration Revocation must be enabled and operational parameters optionally configured.
- **HA service(s):** Registration Revocation must be enabled and operational parameters optionally configured.

Important These instructions assume that the system was previously configured to support subscriber data sessions for a core network service with FA and/or an HA according to the instructions described in the respective product Administration Guide.

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

Configuring FA Services

Configure FA services to support MIP Registration Revocation by applying the following example configuration:

```
configure
   context <context_name>
      fa-service <fa_service_name>
         revocation enable
         revocation max-retransmission <number>
         revocation retransmission-timeout <time>
         end
```

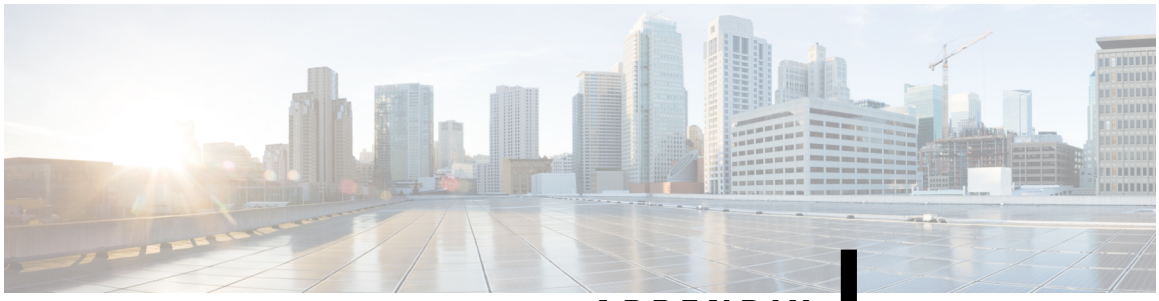
Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring HA Services

Configure HA services to support MIP Registration Revocation by applying the following example configuration:

```
configure
   context <context_name>
      ha-service <ha_service_name>
         revocation enable
         revocation max-retransmission <number>
         revocation retransmission-timeout <time>
         end
```

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*.



APPENDIX L

MSID and PCF Zone Based Call Redirection

This chapter describes MSID and PCF zone based call redirection. 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 the respective product Administration Guide, before using the procedures in this chapter.

Important The MSID and PCF zone based call redirection is a licensed Cisco product. Separate session and feature licenses 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.

Overview

MSID and PCF zone based call redirection allows calls from a specific MSID or a specific PCF zone to be redirected to an alternate PDSN. These features are only applicable to new calls; handoffs are accepted by the PDSN in all cases. If the PDSN is in the process of starting up, the overload policy is applied before the zone/IMSI based call redirection. Once the PDSN is ready to accept new calls, the zone/IMSI based call redirection policy is applied before the overload policy. Upon receiving an RRQ from a PCF, the PDSN sends an RRP with the code 136 - Unknown PDSN Address.

MSID Based Call Redirection

The PDSN contains a table of MSIDs and the corresponding set of PDSNs to which the call should be redirected. It allows the configuration of up to 16 wildcard MSIDs per PDSN service. The wildcard must be a single-digit match represented by the "" character. For example, the MSID 84712 would match all MSIDs starting with 847 followed by any eight digits, followed by 12 and any two additional digits.

When a new call arrives, the PDSN attempts to match the MSID with the configured list of wildcard MSIDs. If a match is found, the call is redirected to one of the PDSNs by IP address using a weighted round-robin algorithm. If more than one match is found, the algorithm selects the match with the longest matching prefix.

PCF Zone Based Call Redirection

Groups of PDSNs maybe configured with a specific numbered zone. When a new call arrives, the PDSN checks the PCF for a specified zone number. If the PCF matches the specified zone, the call is redirected to a PDSN within the zone using a weighted round-robin algorithm. If the PCF from which the call arrived does not belong to a zone, or if no PDSNs are configured for the specified zone, the call is not redirected. Similarly, if a zone is configured for a PCF address and the current PDSN-service address is a member of that zone, the call is not redirected.

Caution These two features introduce additional lookups in the call setup path and could impact the call setup rate.

Important If both MSID and PCF zone based call redirection are configured, MSID based call redirection will have a higher precedence.

Configuring MSID and PCF Zone Based Call Redirection

This section describes the process of setting up MSID and PCF zone based call redirection from the command line interface.

Important Incorrect configuration of the MSID and PCF Zone based Call Redirection features could result in sessions failing to be established. For example, if PDSN1 is configured to redirect sessions to PDSN2 while PDSN2 is configured to redirect sessions to PDSN1, a loop is created in which all sessions would fail to be connected. In addition, sessions will not be established if the PDSN to which the sessions are being redirected is unavailable.

Configuring MSID Based Call Redirection

To configure MSID based call redirection, you must create a new policy that defines a wildcard match list, a list of PDSNs to redirect to, and their respective weights.

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

Configure MSID based call redirection by applying the following example configuration:

```
configure
 context <context_name>
 pdsn-service <pdsn_service_name>
 policy msid-match <msid_with_wildcards> redirect <address>
```

```
weight <weight_num> <address2> weight <weight_num>...<address16> weight <weight_num>
 end
```

Notes:

- You may repeat the **policy msid-match** command as needed, to a maximum of 16 wildcard MSIDs per PDSN service.

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*.

Configuring PCF Zone Based Call Redirection

To configure PCF zone based call redirection, you must create a new policy that defines a zone match list, a list of PDSNs to redirect to, and their respective weights.

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

To configure PCF zone based call redirection:

Step 1 Set parameters by applying the following example configuration:

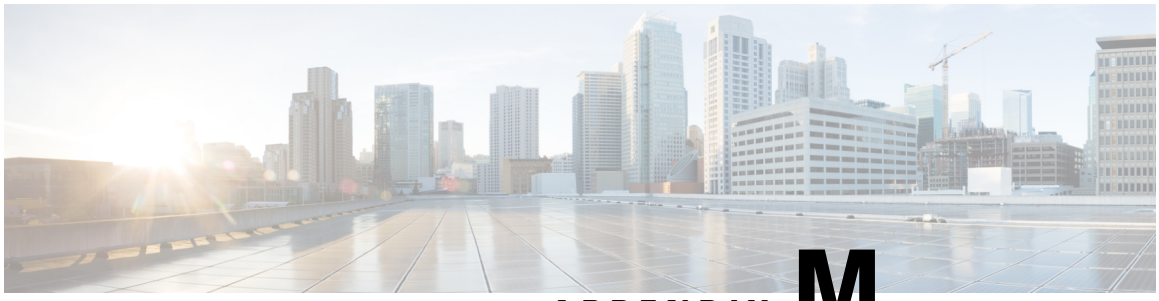
Example:

```
configure
 context <context_name>
 pdsn-service <pdsn_service_name>
 spi remote-address <pcf_ip_address> spi-number <number> secret <secret> zone <zone_id> zone
 <zone_id2>...zone <zone_id32>
 policy pcf-zone-match <zone_number> redirect <address> weight <weight_num> <address2>
weight <weight_num>...<address16>  weight <weight_num>
 end
```

Notes:

- You may repeat the **spi remote-address** <pcf_ip_address> **spi-number** <*number*> **secret** <*secret*> [**zone** <*zone_id*>] [**zone** <*zone_id2*>... **zone** <*zone_id32*>] command as necessary. You can configure up to 32 PCF zones per PDSN service.
- You may repeat the **policy pcf-zone-match** <*zone_number*> { **redirect** <*address*> } [**weight** <*weight_num*>] [<*address2*> [weight <*weight_num*>]...<*address16*> [**weight** <*weight_num*>]] command as necessary, up to a maximum of 32 defined PCF zones and 16 defined PDSNs per PDSN service.

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*



APPENDIX M

Pre-paid Billing

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

This chapter includes the following topics:

Overview

The system supports pre-paid billing for subscriber accounts that use RADIUS Accounting.

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

3GPP2 Standard Pre-paid Billing Overview

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

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

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

Custom Pre-paid Billing Overview

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

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

The system re-authorizes an active subscriber that has used up its byte credits by issuing a RADIUS Access-Request to the RADIUS server. A valid Access-Reject or a RADIUS timeout results in immediate disconnect of the subscriber session. An Access-Accept without attributes that authorize more byte credits allows the subscriber session to continue with the remaining credits. An Access-Accept with attributes containing byte credits results in the addition of these byte credits to the subscriber session, and the continuation of the session until the subscriber session byte credits have been reduced to the low watermark received in the access accept. If not received, it defaults to 10.

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

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

License Requirements

The Pre-paid Billing 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*.

Configuring Standard 3GPP2 Pre-paid Billing

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

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

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

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

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

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

Notes:

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

  prepaid 3gpp2 preference volume

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

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

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

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

  Save the configuration 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*.

Configuring Pre-paid Billing With Custom Behavior

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

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

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

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

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

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

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

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

Notes:

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

  prepaid custom byte-count compressed

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

  prepaid custom low-watermark percent <*percentage*>

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

  prepaid custom renewal interval <*seconds*>

- Save the configuration 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*.

3GPP2 Pre-paid Attributes

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

Attribute	Sub-attribute	Description
3GPP2-Pre-Paid-Acct-Capability		This attribute is for setting the prepaid accounting capability.
	Available-In-Client	The optional Available-In-Client Sub-Type, generated by the PrePaid client, indicates the PrePaid Accounting capabilities of the client in the PDSN or HA and shall be bitmap encoded.
	Selected-For-Session	The optional Selected-For-Session Sub-Type, generated by the PrePaid server, indicates the PrePaid Accounting capability to be used for a given session.
3GPP2-Pre-Paid-Accounting-Quota		This attribute specifies the characteristics for PrePaid accounting of the volume and/or duration of a packet data session. It shall be present in all on-line RADIUS Access-Request and on-line RADIUS Access-Accept messages and may be included in other RADIUS Access-Accept messages. Non-used Sub-Types by the PPC and PPS shall be omitted.
	Quota-Identifier	The Quota-Identifier Sub-Type is generated by the PrePaid server at allocation of a Volume and/or Duration Quota. The on-line quota update RADIUS Access-Request message sent from the PPC to the PPS shall include a previously received Quota-Identifier.

Attribute	Sub-attribute	Description
	Volume-Quota	The optional Volume-Quota Sub-Type is only present if Volume Based charging is used. In RADIUS Access-Accept message (PPS to PPC direction), it indicates the Volume (in octets) allocated for the session by the PrePaid server. In on-line RADIUS Access-Request message (PPC to PPS direction), it indicates the total used volume (in octets) for both forward and reverse traffic applicable to PrePaid accounting13. If a Tariff Switch condition was reached during the session, this Sub-Type contains the complete (before and after) volume used, while the Volume-Used-After-Tariff-Switch attribute contains the volume used after the tariff switch condition.
	Volume-Quota-Overflow	The optional Volume-Quota-Overflow Sub-Type is used to indicate how many times the Volume-Quota counter has wrapped around 232 over the course of the service being provided.
	Volume-Threshold	The Volume-Threshold Sub-Type shall always be present if Volume-Quota is present in a RADIUS Access-Accept message (PPS to PPC direction). It is generated by the PrePaid server and indicates the volume (in octets) that shall be used before requesting quota update. This threshold should not be larger than the Volume-Quota.
	Volume-Threshold-Overflow	The optional Volume-Threshold-Overflow Sub-Type is used to indicate how many times the Volume-Threshold counter has wrapped around 232 over the course of the service being provided.

Attribute	Sub-attribute	Description
	Duration-Quota	The optional Duration-Quota Sub-Type is only present if Duration Based charging is used. In RADIUS Access-Accept message (PPS to PPC direction), it indicates the Duration (in seconds) allocated for the session by the PrePaid server. In on-line RADIUS Access-Accept message (PPC to PPS direction), it indicates the total Duration (in seconds) since the start of the accounting session related to the Quota-ID.
	Duration-Threshold	The Duration-Threshold Sub-Type shall always be present if Duration-Quota is present in a RADIUS Access-Accept message (PPS to PPC direction). It represents the duration (in seconds) that shall be used by the session before requesting quota update. This threshold should not be larger than the Duration-Quota and shall always be sent with the Duration-Quota.
	Update-Reason	The Update-Reason Sub-Type shall be present in the on-line RADIUS Access-Request message (PPC to PPS direction). It indicates the reason for initiating the on-line quota update operation. Update reasons 4, 5, 6, 7 and 8 indicate that the associated resources are released at the client side, and therefore the PPS shall not allocate a new quota in the RADIUS Access-Accept message.

Attribute	Sub-attribute	Description
	Pre-Paid-Server	The optional, multi-value PrePaid-Server indicates the address of the serving PrePaid System. If present, the Home RADIUS server uses this address to route the message to the serving PrePaid Server. The attribute may be sent by the Home RADIUS server. If present in the incoming RADIUS Access-Accept message, the PDSN shall send this attribute back without modifying it in the subsequent RADIUS Access-Request message, except for the first one. If multiple values are present, the PDSN shall not change the order of the attributes.

These attributes can be found in the following dictionaries:

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

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

Pre-paid Attributes

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

Attribute	Description
SN-Prepaid-Inbound-Octets	If only SN-Prepaid-Inbound-Octets is in the Access-Accept, and the others are not, then the number of outbound credits is infinite.
SN-Prepaid-Outbound-Octets	If only SN-Prepaid-Outbound-Octets is in the Access-Accept, and the others are not, then the number of inbound credits is infinite.
SN-Prepaid-Total-Octets	If only SN-Prepaid-Total-Octets is in the Access-Accept, and the others are not, then pre-paid credits is only enforced on the total byte throughput.

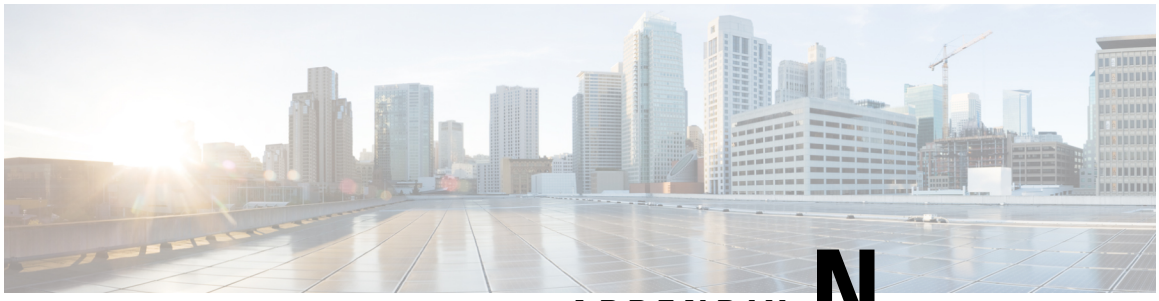
Attribute	Description
SN-Prepaid-Timeout	SN-Prepaid-Timeout can be used alone or in combination with the other attributes. This integer RADIUS attribute includes a time limit in seconds. Regardless of the values of the Octet counters, the session should send a new authorization request upon timer expiration.
SN-Prepaid-Watermark	SN-Prepaid-Watermark is optional with any of the attributes. If it is not included it defaults to the CLI default subscriber configuration, which defaults to a value of 10. This watermark applies to any of the pre-paid attributes being enforced.

These attributes can be found in the following dictionaries:

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

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

Pre-paid Billing



APPENDIX N

Rejection/Redirection of HA Sessions on Network Failures

This chapter provides information on configuring an enhanced, or extended, service. 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 the respective product Administration Guide, before using the procedures in this chapter.

This chapter contains the following topics:

Overview

This feature enables the HA service to either reject new calls or redirect them to another HA when a destination network connection failure is detected. When network connectivity is re-established, the HA service begins to accept calls again in the normal manner.

The way this is implemented in the system is as follows:

- A policy is configured in the HA service that tells the service what action to take when network connectivity is lost. New calls are either directed to one of up to 16 different IP addresses or all new calls are rejected until network connectivity is restored.
- In the destination context, a network reachability server is configured. This is a device on the destination network to which ping packets are periodically sent to determine if the network is reachable. As soon as a network reachability server is configured, pinging of the server commences whether or not the server name is bound to a subscriber or an IP pool.
- The name of the network reachability server configured in the destination context is bound to either a local subscriber profile or an IP pool. If the subscriber is authenticated by an AAA server, RADIUS attributes may specify the network reachability server for the subscriber. (If an IP pool has a network reachability server name bound to it, that takes precedence over both the RADIUS attributes and the local subscriber configuration.)

Configuring HA Session Redirection

This section provides instructions for configuring rejection or redirection of HA sessions on the event of a network failure. These instructions assume that there is a destination context. and HA service, an IP pool, and a subscriber already configured and that you are at the root prompt for the Exec mode:

```
[local]host_name
```

Step 1 Enter the global configuration mode by entering the following command:

configure

The following prompt appears:

```
[local]host_name(config)
```

Step 2 Enter context configuration mode by entering the following command:

context <*context_name*>

context_name is the name of the destination context where the HA service is configured. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive.The following prompt appears:

```
[<context_name>]host_name(config-ctx)
```

Step 3 Enter the HA service configuration mode by entering the following command:

ha-service <*ha_service_name*>

ha_service_name is the name of the HA service. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive.The following prompt appears:

```
[<context_name>]host_name(config-ha-service)
```

Step 4 Configure the action for the HA service to take when network connectivity is lost by entering the following command:

policy nw-reachability-fail { reject [use-reject-code { admin-prohibited | insufficient-resources }] | redirect <*ip_addr1*> [**weight** <*value*>] [<*ip_addr2*> [**weight** <*value*>]] ... [<*ip_addr16*> [**weight** <*value*>]] }

Keyword/Variable	Description
reject	Upon network reachability failure reject all new calls for this context.
use-reject-code { admin-prohibited | insufficient-resources }	When rejecting calls send the specified reject code. If this keyword is not specified the admin-prohibited reject code is sent by default.

Keyword/Variable	Description
redirect <*ip_addr1*> [**weight** <*value*>] [<*ip_addr2*> [**weight** <*value*>]] ... [<*ip_addr16*> [**weight** <*value*>]]	Upon network reachability failure redirect all calls to the specified IP address. <*ip_addr*>: This must be an IPv4 address. Up to 16 IP addresses and optional weight values can be entered on one command line. **weight** <*value*>: When multiple addresses are specified, they are selected in a weighted round-robin scheme. If a weight is not specified, the entry is automatically assigned a weight of 1. <*value*> must be an integer from 1 through 10.

Step 5 Enter the following command to return to the context configuration mode:

exit

The following prompt appears:

[<*context_name*>]*host_name***(config-ctx)**

Step 6 Specify the network device on the destination network to which ping packets should be sent to test for network reachability, by entering the following command:

nw-reachability server <*server_name*> [**interval** <*seconds*>] [**local-addr** <*ip_addr*>] [**num-retry** <*num*>] [**remote-addr** <*ip_addr*>] [**timeout** < *seconds*>]

Keyword/Variable	Description
server_name	A name for the network device that is sent ping packets to test for network reachability.
interval <*seconds*>	Default: 60 seconds Specifies the frequency in seconds for sending ping requests.<*seconds*> must be an integer from 1 through 3600.
local-addr <*ip_addr*>	Specifies the IP address to be used as the source address of the ping packets; If this is unspecified, an arbitrary IP address that is configured in the context is used. <*ip_addr*> must be an IP v4 address.
num-retry <*num*>	Default: 5 Specifies the number of retries before deciding that there is a network-failure. <*num*> must be an integer from 0 through 100.
remote-addr <*ip_addr*>	Specifies the IP address of a network element to use as the destination to send the ping packets for detecting network failure or reachability. <*ip_addr*> must be an IPv4 address.

Keyword/Variable	Description
timeout < *seconds*>	Default: 3 seconds Specifies how long to wait, in seconds, before retransmitting a ping request to the remote address. <*seconds*> must be an integer from 1 through 10.

Step 7 Repeat *step 6* to configure additional network reachability servers.

Step 8 To bind a network reachability server to an IP pool, continue with *step 9*. To bind a network reachability server to a local subscriber profile, skip to *step 11*.

Step 9 To bind a network reachability server name to an IP pool, enter the following command:

ip pool <*pool_name*> **nw-reachability server** <*server_name*>

<*pool_name*>	The name of an existing IP pool in the current context.
nw-reachability server <*server_name*>	Bind the name of a configured network reachability server to the IP pool and enable network reachability detection for the IP pool. This takes precedence over any network reachability server settings in a subscriber configuration or RADIUS attribute. <*server_name*>: The name of a network reachability server that has been defined in the current context. This is a string of from 1 through 16 characters.

Step 10 Repeat *step 9* for additional IP pools in the current context then skip to *step 13*.

Step 11 Enter the subscriber configuration mode by entering the following command:

subscriber { default | name <*subs_name*> }

Where **default** is the default subscriber for the current context and *subs_name* is the name of the subscriber profile that you want to configure for network reachability.The following prompt appears:

[<*context_name*>]*host_name***(config-subscriber)**

Step 12 To bind a network reachability server name to the current subscriber in the current context, enter the following command:

nw-reachability server <*server_name*>

Where *server_name* is the name of a network reachability server that has been defined in the current context.

Step 13 Return to the executive mode by entering the following command:

end

The following prompt appears:

[local]*host_name*

Step 14 Enter the executive mode for the destination context for which you configured network reachability by entering the following command:

context <*context_name*>

Where *context_name* is the name of the destination context for which you configured network reachability.The following prompt appears:

```
[context_name]host_name
```

Step 15 Check the network reachability server configuration by entering the following command

show nw-reachability server all

The output of this command appears similar to the following:

```
  Server           remote-addr     local-addr      state
 ---------------  --------------- --------------- ---------------
 nw-server1       192.168.100.20  192.168.1.10    Down
  Total Network Reachability Servers: 1 Up: 0
```

Ensure that the remote and local addresses are correct. The state column indicates whether or not the server is reachable (Up) or unreachable (Down).

Step 16 Check the HA service policy by entering the following command:

show ha-service name <*ha_service_name*>

Where <*ha_service_name*> is the name of the HA service in the current context for which you configured a network reachability policy.The output of this command includes information about the network reachability policy that looks similar to the following:

```
NW-Reachability Policy:  Reject    (Reject code: Admin Prohibited)
```

Step 17 Check the network reachability server name bound to an IP pool by entering the following command:

show ip pool pool-name <*pool_name*>

Where <*pool_name*> is the name of the IP pool to which you bound a network reachability server name.The output of this command includes information about the network reachability server name that looks similar to the following:

```
Network Reachability Detection Server: nw-server1
```

Step 18 Check the network reachability server name bound to a local subscriber profile by entering the following command:

show subscribers configuration username <*subscriber_name*>

Where <*subscriber_name*> is the name of the local subscriber to which you bound a network reachability server name.The output of this command includes information about the network reachability server name that looks similar to the following:

```
network reachability detection server name: nw-server1
```

Step 19 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*.

RADIUS Attributes

Attributes defined in a subscriber profile stored remotely on a RADIUS server can be used to bind the network reachability server to a subscriber session. Use the following attributes to bind a network reachability server to a subscriber session;

- **SN-Nw-Reachability-Server-Name**
- **SN1-Nw-Reachability-Server-Name**

Rejection/Redirection of HA Sessions on Network Failures

The attributes have one possible value, which is a variable that is a string of from 1 to 15 characters in length. This should be the name of the configured network reachability server.

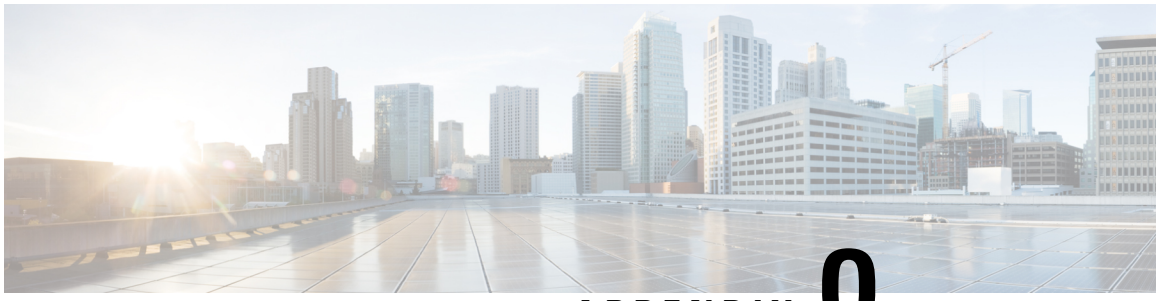
The **SN-Nw-Reachability-Server-Name** attribute is contained in the following dictionaries:

- starent
- starent-835

The **SN1-Nw-Reachability-Server-Name** attribute is contained in the following dictionaries:

- starent-vsa1
- starent-vsa1-835

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



APPENDIX O

Traffic Policing and Shaping

This chapter describes the support of per subscriber Traffic Policing and Shaping feature on Cisco's Chassis and explains the commands and RADIUS attributes that are used to implement this feature. 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 the respective product Administration Guide, before using the procedures in this chapter.

Important Traffic Policing and Shaping 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*.

The following topics are included:

Overview

This section describes the traffic policing and shaping feature for individual subscriber. This feature is comprises of two functions:

- Traffic Policing
- Traffic Shaping

Traffic Policing

Traffic policing enables the configuring and enforcing of bandwidth limitations on individual subscribers and/or APN of a particular traffic class in 3GPP/3GPP2 service.

Bandwidth enforcement is configured and enforced independently on the downlink and the uplink directions.

A Token Bucket Algorithm (a modified trTCM) [RFC2698] is used to implement the Traffic-Policing feature. The algorithm used measures the following criteria when determining how to mark a packet:

- **Committed Data Rate (CDR):** The guaranteed rate (in bits per second) at which packets can be transmitted/received for the subscriber during the sampling interval.
- **Peak Data Rate (PDR):** The maximum rate (in bits per second) that subscriber packets can be transmitted/received for the subscriber during the sampling interval.
- **Burst-size:** The maximum number of bytes that can be transmitted/received for the subscriber during the sampling interval for both committed (CBS) and peak (PBS) rate conditions. This represents the maximum number of tokens that can be placed in the subscriber's "bucket". Note that the committed burst size (CBS) equals the peak burst size (PBS) for each subscriber.

The system can be configured to take any of the following actions on packets that are determined to be in excess or in violation:

- **Drop:** The offending packet is discarded.
- **Transmit:** The offending packet is passed.
- **Lower the IP Precedence:** The packet's ToS bit is set to "0", thus downgrading it to Best Effort, prior to passing the packet. Note that if the packet's ToS bit was already set to "0", this action is equivalent to "Transmit".

Traffic Shaping

Traffic Shaping is a rate limiting method similar to the Traffic Policing, but provides a buffer facility for packets exceeded the configured limit. Once the packet exceeds the data-rate, the packet queued inside the buffer to be delivered at a later time.

The bandwidth enforcement can be done in the downlink and the uplink direction independently. If there is no more buffer space available for subscriber data system can be configured to either drop the packets or kept for the next scheduled traffic session.

Important Traffic Shaping is not supported on the GGSN, P-GW, or SAEGW.

Traffic Policing Configuration

Traffic Policing is configured on a per-subscriber basis. The subscribers can either be locally configured subscribers on the system or subscriber profiles configured on a remote RADIUS server.

In 3GPP service Traffic policing can be configured for subscribers through APN configuration as well.

Important In 3GPP service attributes received from the RADIUS server supersede the settings in the APN.

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

Configuring Subscribers for Traffic Policing

Important Instructions for configuring RADIUS-based subscriber profiles are not provided in this document. Please refer to the documentation supplied with your server for further information.

Step 1 Configure local subscriber profiles on the system to support Traffic Policing by applying the following example configurations:

a) To apply the specified limits and actions to the downlink (data to the subscriber):

```
configure
    context <context_name>
        subscriber name <user_name>
            qos traffic-police direction downlink
            end
```

b) To apply the specified limits and actions to the uplink (data from the subscriber):

```
configure
    context <context_name>
        subscriber name <user_name>
            qos traffic-police direction uplink
            end
```

Notes:

- There are numerous keyword options associated with the **qos traffic-police direction { downlink | uplink }** command.
- Repeat for each additional subscriber to be configured.

Note If the exceed/violate action is set to "lower-ip-precedence", the TOS value for the outer packet becomes "best effort" for packets that exceed/violate the traffic limits regardless of what the **ip user-datagram-tos-copy** command in the Subscriber Configuration mode is configured to. In addition, the "lower-ip-precedence" option may also override the configuration of the **ip qos-dscp** command (also in the Subscriber Configuration mode). Therefore, it is recommended that command not be used when specifying this option.

Step 2 Verify the subscriber profile configuration by applying the following example configuration:

```
context <context_name>
    show subscriber configuration username <user_name>
```

Step 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*.

Configuring APN for Traffic Policing in 3GPP Networks

This section provides information and instructions for configuring APN template's QoS profile in support of Traffic Policing.

The profile information is sent to the SGSN(s) in response to GTP Create/Update PDP Context Request messages. If the QoS profile requested by the SGSN is lower than the configured QoS profile configured, the profile requested by the SGSN is used. If the QoS profile requested by the SGSN is higher, the configured rates are used.

Note that values for the committed-data-rate and peak-data-rate parameters are exchanged in the GTP messages between the GGSN and the SGSN. Therefore, the values used may be lower than the configured values. When negotiating the rate with the SGSN(s), the system convert this to a value that is permitted by GTP as shown in the table below.

Table 31: Permitted Values for Committed and Peak Data Rates in GTP Messages

Value (bps)	Increment Granularity (bps)
From 1000 to 63,000	1,000 (e.g 1000, 2000, 3000, ... 63000)
From 64,000 to 568,000	8,000 (e.g. 64000, 72000, 80000, ... 568000)
From 576,000 to 8,640,000	64,000 (e.g. 576000, 640000, 704000, ... 86400000)
From 8,700,000 to 16,000,000	100,000 bps (e.g. 8700000, 8800000, 8900000, ... 16000000)

Step 1 Set parameters by applying the following example configurations:

a) To apply the specified limits and actions to the downlink (the Gn direction):

```
configure
    context <context_name>
        apn <apn_name>
            qos rate-limit downlink
            end
```

b) To apply the specified limits and actions to the uplink (the Gi direction):

```
configure
    context <context_name>
        apn <apn_name>
            qos rate-limit uplink
            end
```

Notes:

- There are numerous keyword options associated with **qos rate-limit { downlink | uplink }** command.

- *Optionally*, configure the maximum number of PDP contexts that can be facilitated by the APN to limit the APN's bandwidth consumption by entering the following command in the configuration:

  max-contents primary *<number>* **total** *<total_number>*

- Repeat as needed to configure additional Qos Traffic Policing profiles.

Important If a "subscribed" traffic class is received, the system changes the class to background and sets the following: The uplink and downlink guaranteed data rates are set to 0. If the received uplink or downlink data rates are 0 and traffic policing is disabled, the default of 64 kbps is used. When enabled, the APN configured values are used. If the configured value for downlink max data rate is larger than can fit in an R4 QoS profile, the default of 64 kbps is used. If either the received uplink or downlink max data rates is non-zero, traffic policing is employed if enabled for the background class. The received values are used for responses when traffic policing is disabled.

Step 2 Verify that your APNs were configured properly by entering the following command:

```
show apn { all | name <apn_name> }
```

The output is a concise listing of configured APN parameter settings.

Step 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*.

Traffic Shaping Configuration

Traffic Shaping is configured on a per-subscriber basis. The subscribers can either be locally configured subscribers on the system or subscriber profiles configured on a remote RADIUS server.

In 3GPP service Traffic policing can be configured for subscribers through APN configuration as well.

Important In 3GPP, service attributes received from the RADIUS server supersede the settings in the APN.

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

Important Traffic Shaping is not supported on the GGSN, P-GW, or SAEGW.

Configuring Subscribers for Traffic Shaping

This section provides information and instructions for configuring local subscriber profiles on the system to support Traffic Shaping.

Important Instructions for configuring RADIUS-based subscriber profiles are not provided in this document. Please refer to the documentation supplied with your server for further information.

Step 1 Set parameters by applying the following example configurations:

a) To apply the specified limits and actions to the downlink (data to the subscriber):

```
configure
    context <context_name>
        subscriber name <user_name>
            qos traffic-shape direction downlink
            end
```

b) To apply the specified limits and actions to the uplink (data to the subscriber):

```
configure
    context <context_name>
        subscriber name <user_name>
            qos traffic-shape direction uplink
            end
```

Notes:

- There are numerous keyword options associated with **qos traffic-shape direction { downlink | uplink }** command.
- Repeat for each additional subscriber to be configured.

Important If the exceed/violate action is set to "lower-ip-precedence", the TOS value for the outer packet becomes "best effort" for packets that exceed/violate the traffic limits regardless of what the **ip user-datagram-tos-copy** command in the Subscriber Configuration mode is configured to. In addition, the "lower-ip-precedence" option may also override the configuration of the **ip qos-dscp** command (also in the Subscriber Configuration mode). Therefore, it is recommended that command not be used when specifying this option.

Step 2 Verify the subscriber profile configuration by applying the following example configuration:

```
context <context_name>
    show subscriber configuration username <user_name>
```

Step 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*.

Configuring APN for Traffic Shaping in 3GPP Networks

This section provides information and instructions for configuring APN template's QoS profile in support of Traffic Shaping.

The profile information is sent to the SGSN(s) in response to GTP Create/Update PDP Context Request messages. If the QoS profile requested by the SGSN is lower than the configured QoS profile configured, the profile requested by the SGSN is used. If the QoS profile requested by the SGSN is higher, the configured rates are used.

Note that values for the committed-data-rate and peak-data-rate parameters are exchanged in the GTP messages between the GGSN and the SGSN. Therefore, the values used may be lower than the configured values. When negotiating the rate with the SGSN(s), the system convert this to a value that is permitted by GTP as shown in the following table.

Table 32: Permitted Values for Committed and Peak Data Rates in GTP Messages 0

Value (bps)	Increment Granularity (bps)
From 1000 to 63,000	1,000 (e.g 1000, 2000, 3000, ... 63000)
From 64,000 to 568,000	8,000 (e.g. 64000, 72000, 80000, ... 568000)
From 576,000 to 8,640,000	64,000 (e.g. 576000, 640000, 704000, ... 86400000)
From 8,700,000 to 16,000,000	100,000 bps (e.g. 8700000, 8800000, 8900000, ... 16000000)

Step 1 Set parameters by applying the following example configurations.

a) To apply the specified limits and actions to the downlink (data to the subscriber):

```
configure
    context <context_name>
        subscriber name <user_name>
            qos rate-limit downlink
            end
```

b) To apply the specified limits and actions to the uplink (data to the subscriber):

```
configure
    context <context_name>
        apn <apn_name>
            qos rate-limit uplink
            end
```

Step 2 Verify that your APNs were configured properly by entering the following command:

```
show apn { all | name <apn_name> }
```

The output is a concise listing of configured APN parameter settings.

Step 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*.

RADIUS Attributes

Traffic Policing for CDMA Subscribers

The RADIUS attributes listed in the following table are used to configure Traffic Policing for CDMA subscribers (PDSN, HA) configured on remote RADIUS servers. More information on these attributes can be found in the *AAA Interface Administration and Reference*.

Table 33: RADIUS Attributes Required for Traffic Policing Support for CDMA Subscribers

Attribute	Description
SN-QoS-Tp-Dnlk (or SN1-QoS-Tp-Dnlk)	Enable/disable traffic policing in the downlink direction.
SN-Tp-Dnlk-Committed-Data-Rate (or SN1-Tp-Dnlk-Committed-Data-Rate)	Specifies the downlink committed-data-rate in bps.
SN-Tp-Dnlk-Peak-Data-Rate (or SN1-Tp-Dnlk-Committed-Data-Rate)	Specifies the downlink peak-data-rate in bps.
SN-Tp-Dnlk-Burst-Size (or SN1-Tp-Dnlk-Burst-Size)	Specifies the downlink-burst-size in bytes. **NOTE:** It is recommended that this parameter be configured to at least the greater of the following two values: 1) 3 times greater than packet MTU for the subscriber connection, OR 2) 3 seconds worth of token accumulation within the "bucket" for the configured peak-data-rate.
SN-Tp-Dnlk-Exceed-Action (or SN1-Tp-Dnlk-Exceed-Action)	Specifies the downlink exceed action to perform.
SN-Tp-Dnlk-Violate-Action (or SN1-Tp-Dnlk-Violate-Action)	Specifies the downlink violate action to perform.
SN-QoS-Tp-Uplk (or SN1-QoS-Tp-Uplk)	Enable/disable traffic policing in the downlink direction.
SN-Tp-Uplk-Committed-Data-Rate (or SN1-Tp-Uplk-Committed-Data-Rate)	Specifies the uplink committed-data-rate in bps.

Attribute	Description
SN-Tp-Uplk-Peak-Data-Rate (or SN1-Tp-Uplk-Committed-Data-Rate)	Specifies the uplink peak-data-rate in bps.
SN-Tp-Uplk-Burst-Size (or SN1-Tp-Uplk-Burst-Size)	Specifies the uplink-burst-size in bytes. **Note** It is recommended that this parameter be configured to at least the greater of the following two values: 1) 3 times greater than packet MTU for the subscriber connection, OR 2) 3 seconds worth of token accumulation within the "bucket" for the configured peak-data-rate.
SN-Tp-Uplk-Exceed-Action (or SN1-Tp-Uplk-Exceed-Action)	Specifies the uplink exceed action to perform.
SN-Tp-Uplk-Violate-Action (or SN1-Tp-Uplk-Violate-Action)	Specifies the uplink violate action to perform.

Traffic Policing for UMTS Subscribers

The RADIUS attributes listed in the following table are used to configure Traffic Policing for UMTS subscribers configured on remote RADIUS servers. More information on these attributes can be found in the *AAA Interface Administration and Reference*.

Table 34: RADIUS Attributes Required for Traffic Policing Support for UMTS Subscribers

Attribute	Description
SN-QoS-Conversation-Class (or SN1-QoS-Conversation-Class)	Specifies the QOS Conversation Traffic Class.
SN-QoS-Streaming-Class (or SN1-QoS-Streaming-Class)	Specifies the QOS Streaming Traffic Class.
SN-QoS-Interactive1-Class (or SN1-QoS-Interactive1-Class)	Specifies the QOS Interactive Traffic Class.
SN-QoS-Interactive2-Class (or SN1-QoS-Interactive2-Class)	Specifies the QOS Interactive2 Traffic Class.
SN-QoS-Interactive3-Class (or SN1-QoS-Interactive3-Class)	Specifies the QOS Interactive3 Traffic Class.
SN-QoS-Background-Class (or SN1-QoS-Background-Class)	Specifies the QOS Background Traffic Class.

Attribute	Description
SN-QoS-Traffic-Policy (or SN1-QoS-Traffic-Policy)	This compound attribute simplifies sending QoS values for Traffic Class (the above attributes), Direction, Burst-Size, Committed-Data-Rate, Peak-Data-Rate, Exceed-Action, and Violate-Action from the RADIUS server. This attribute can be sent multiple times for different traffic classes. If Class is set to 0, it applies across all traffic classes.